Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2026

Audit Report • AUD-2026-004 • July 30, 2026

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency
400 7th Street SW, Washington, DC 20219

July 30, 2026

TO: Jeffery Harris, Acting Deputy Chief Operating Officer, Chief Information Officer, and Chief Information Security Officer

FROM: James Hodge, Deputy Inspector General for Audits /s/

SUBJECT: Audit Report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2026* (AUD-2026-004)

We are pleased to transmit the subject report.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, among other things, to develop, document, and implement agency-wide information security programs and practices to protect information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, federal agencies must undergo an annual independent evaluation of their information security programs and practices to determine the effectiveness of such program and practices.

Pursuant to FISMA, we contracted with Sikich CPA LLC (herein referred to as "Sikich"), a certified independent public accounting firm, to conduct the fiscal year (FY) 2026 independent evaluation of the Agency's (collectively, the Federal Housing Finance Agency (FHFA) and the FHFA Office of Inspector General (OIG)) information security programs and practices. Sikich conducted its evaluation as a performance audit under generally accepted government auditing standards. The objectives of this performance audit were to: (1) evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the FY 2025 Inspector General FISMA Reporting Metrics.[1] Sikich reviewed selected controls mapped to these metrics for a sample of information systems in the Agency's FISMA inventories of reportable information systems.

Sikich concluded that, while the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines, the Agency's information security programs

[1] On March 17, 2026, the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency issued a joint communication noting that in order to meet the FISMA independent evaluation requirements, IGs and independent external auditors are directed to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits.

and practices were not effective. Specifically, the Agency is at an overall maturity Level 2 – *Defined.* Sikich identified 2 new weaknesses in 4 of the 6 Cybersecurity Functions and within 4 of the 10 IG FISMA Metric domains. To address these weaknesses, Sikich made four new recommendations to assist the Agency in strengthening its information security programs and practices and noted five open recommendations from prior audits.

In connection with the contract, we reviewed Sikich's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to conclude, and we do not conclude, on the effectiveness of the Agency's implementation of its information security programs and practices and compliance with FISMA and related information security policies, procedures, standards, and guidelines. Sikich is responsible for the attached auditor's report dated July 22, 2026, and the conclusions expressed therein. Our review found no instances where Sikich did not comply, in all material respects, with generally accepted government auditing standards.

As discussed in Sikich's report, the Agency's management did not agree with the recommendations.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Information Security Programs and Practices
Fiscal Year 2026

SIKICH®

Federal Housing Finance Agency (FHFA)

Performance Audit of FHFA's Information Security Programs and Practices for 2026

Performance Audit Report

JULY 22, 2026

sikich.com

SIKICH

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

July 22, 2026

Christian J. Schrank
Acting Principal Deputy, Performing the Duties of the Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Mr. Schrank:

Sikich CPA LLC (Sikich) conducted a performance audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG), collectively referred to as the Agency for reporting combined results, information security programs and practices for the 12 months ending on March 31, 2026, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program. FISMA also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and practices. We performed this audit under contract with the FHFA-OIG.

The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the *Fiscal Year (FY) 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (IG FISMA Reporting Metrics).[1] The audit covered the period from April 1, 2025, through March 31, 2026. We conducted audit fieldwork remotely and onsite at the Agency's headquarters in Washington DC, from October 2025 through June 2026.

We conducted this performance audit 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. We describe our objectives, scope, and methodology in **Appendix II: Objective, Scope, and Methodology.**

We appreciate the assistance we received from the Agency. We will be pleased to discuss any questions you may have regarding the contents of this report.

Sincerely,

Sikich CPA LLC

[1] On March 17, 2026, Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency issued a joint communication directing IGs and independent external auditors to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits.

Table of Contents

1.0 Executive Summary 1
2.0 Audit Results 3
3.0 Audit Findings 8
1. FHFA Did Not Conduct and Document Annual Security Control Assessments. 8
2. FHFA Did Not Disable Inactive Privileged User Accounts for a Cloud System in a Timely Manner, and the Cloud System's User Re-authorization Review Did Not Identify Inactive Accounts. 10
4.0 Evaluation of Management Comments 13
Appendix I: Background 17
Appendix II: Objective, Scope, and Methodology 20
Appendix III: Status of Prior Recommendations 24
Appendix IV: Management's Comments 29

1.0 Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged Sikich CPA LLC (Sikich) to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of FHFA's and FHFA-OIG's (collectively referred to as the Agency for reporting combined results) information security programs and practices. The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the *Fiscal Year (FY) 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (IG FISMA Reporting Metrics).[2]

OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for preparing annual FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*[3] which provides reporting guidance for FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the IG FISMA Reporting Metrics.

The IG FISMA Reporting Metrics require us to assess the maturity of six Cybersecurity Framework (CSF) functions[4] in the Agency's information security programs and practices. For

[2] On March 17, 2026, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), issued a joint communication directing IGs and independent external auditors to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits. See the IG FISMA Reporting Metrics online here.

[3] For FY 2026, OMB and DHS did not issue the annual FISMA instructions; therefore, we performed the audit using OMB Memorandum M-25-04*, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements.* See OMB Memorandum M-25-04 online here.

[4] The IG FISMA Reporting Metrics align with the six functions in the NIST Cybersecurity Framework 2.0 (Cybersecurity Framework): *Govern, Identify, Protect, Detect, Respond, and Recover*. The CSF provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

this year's review, IGs were required to assess 20 core[5] and 5 supplemental[6] IG FISMA Reporting Metrics across six function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agencies' information security program and the maturity level of each function area.[7] The maturity levels are Level 1 – *Ad Hoc*, Level 2 – *Defined*, Level 3 – *Consistently Implemented*, Level 4 – *Managed and Measurable*, and Level 5 – *Optimized*. To be considered effective, an agency's information security program must be rated Level 4 – *Managed and Measurable* or higher. See **Appendix I** for additional information on the IG FISMA Reporting Metrics and FISMA reporting requirements.

The scope of this performance audit included the Agency's information security programs and practices covering the period from April 1, 2025, through March 31, 2026. We conducted audit fieldwork remotely and onsite at the Agency's headquarters in Washington DC, from October 2025 through June 2026.

For this audit, Sikich reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the IG FISMA Reporting Metrics, for a sample of Agency information systems[8] in the Agency's FISMA inventories of information systems.

We concluded that the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines. However, we determined that the Agency's information security programs and practices were not effective. Specifically, the Agency is at an overall Level 2 – *Defined* maturity level. In this audit, we identified 2 weaknesses in 4 of 6 CSF functions, and within 4 of the 10 IG FISMA Reporting Metric domains. As a result, we made 4 recommendations to assist the Agency in strengthening its information security programs and practices.

We conducted this performance audit 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.

[5] Core metrics are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the IG FISMA Reporting Metrics online here.

[6] Supplemental metrics are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. The supplemental metrics can be found in the IG FISMA Reporting Metrics online here.

[7] The function areas are further broken down into ten domains (Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning).

[8] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2.0 Audit Results

Progress Since 2025

At the beginning of our performance audit, there were 17 open recommendations from prior FISMA and Privacy audits (1 from the FY 2020 FISMA audit, 2 from the FY 2023 FISMA audit, 5 from the 2024 FISMA audit, 6 from the 2025 FISMA audit, and 3 from the 2025 Privacy audit).

During this audit, the Agency took corrective actions to address 12 of these recommendations, and we consider them closed. Corrective actions are in progress on the other five open recommendations that directly impacted the current-year metrics. Refer to **Appendix III** for a detailed description and status of each recommendation.

Current Status

We concluded that the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines. However, we determined that the Agency's information security programs were not effective. Specifically, we noted that two CSF functions achieved a maturity of Level 3 – *Consistently Implemented* and four CSF functions achieved a maturity of Level 2 – *Defined*. Since none of the six CSF functions reached Level 4 – *Managed and Measurable*, the Agency's information security programs did not meet the criteria for effectiveness. As a result, the Agency's overall maturity was rated as Level 2 – *Defined* (Not Effective). **Table 1** shows a summary of the overall maturity levels for each function and domain in the IG FISMA Reporting Metrics.

Table 1: Maturity Levels for IG FISMA Reporting Metrics

CSF Functions[9]	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 3: Consistently Implemented (Not Effective)	Cybersecurity Governance	Level 3: Consistently Implemented (Not Effective)
		Cybersecurity Supply Chain Risk Management	Level 3: Consistently Implemented (Not Effective)
Identify	Level 2: Defined (Not Effective)	Risk and Asset Management	Level 2: Defined (Not Effective)
Protect	Level 2: Defined (Not Effective)	Configuration Management	Level 2: Defined (Not Effective)
		Identity and Access Management	Level 2: Defined (Not Effective)
		Data Protection and Privacy	Level 2: Defined (Not Effective)
		Security Training	Level 5: Optimized (Effective)
Detect	Level 2: Defined (Not Effective)	Information Security Continuous Monitoring	Level 2: Defined (Not Effective)
Respond	Level 3: Consistently Implemented (Not Effective)	Incident Response	Level 3: Consistently Implemented (Not Effective)
Recover	Level 2: Defined (Not Effective)	Contingency Planning	Level 2: Defined (Not Effective)
Overall	**Level 2: Defined (Not Effective)**		

Source: Sikich's analysis of the Agency's maturity levels for the IG FISMA Reporting Metrics.

[9] See Appendix I, Tables 3 and 4, for definitions and explanations of the CSF functions and domains and maturity levels, respectively.

We found that the Agency established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the Agency:

- Completed a review and update of System Security Plans (SSPs) and Customer Control Plans.
- Established a CSF implementation plan and developed current and target profiles.
- Implemented policies and procedures to monitor background reinvestigation processes.

In addition, the Agency made progress in implementing prior-year FISMA and Privacy audit recommendations. Notwithstanding these actions, the overall maturity level reflects the continued impact of the remaining open recommendations that directly affect the current-year IG FISMA Reporting Metrics. When coupled with new findings identified during the current-year audit and other data sources and risk factors (e.g., relevant FHFA-OIG audits), these factors had a more pronounced impact on the overall maturity level determination. In addition, the overall maturity level reflects the Agency's performance against the current IG FISMA Reporting Metrics, which focus on a streamlined set of core and supplemental metrics. Therefore, the Agency must make further improvements in its information security for the programs to be effective.

As a result, in accordance with the IG FISMA Reporting Metrics guidance,[10] we considered the calculated average scores of the core and supplemental IG FISMA Reporting Metrics, together with the progress made addressing outstanding prior-year FISMA and Privacy audit recommendations, and other data sources or risk indicators (e.g., relevant FHFA-OIG audits) to come to this risk-based conclusion. In conclusion, we rated the Agency's overall maturity level as Level 2 – *Defined* (Not Effective).

This report describes areas where continued attention is needed to strengthen the effectiveness of the Agency's information security programs. Specifically, in this audit, we identified two weaknesses in the Cybersecurity Governance, Risk and Asset Management, Identity and Access Management, and the Information Security Continuous Monitoring domains of the IG FISMA Reporting Metrics (see Findings 1 and 2 in **Table 2**). As such, we made four recommendations to assist the Agency in strengthening its information security programs and practices. These weaknesses, in combination with prior-year open FISMA and relevant FHFA-OIG audit recommendations and weaknesses noted in relevant FHFA-OIG audits,[11] significantly impacted the Agency's overall information security programs and practices. Specifically, the Agency needs to improve controls over Cybersecurity Governance, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Information Security Continuous Monitoring, Incident Response, and Contingency

[10] The IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on their evaluations. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity lower than Level 4.

[11] The following FHFA-OIG audits that impacted the IG FISMA Reporting Metrics were taken into consideration: *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement* (September 25, 2024) (AUD-2024-010), *Vulnerabilities in FHFA's Public Facing Systems Risk Unauthorized Access To Non-Public Data* (September 25, 2025) (AUD-2025-007), and FHFA-OIG's ongoing internal penetration test of FHFA's network and systems (Assignment No. OA-26-003).

Planning. **Table 2** below maps weaknesses to IG FISMA Reporting Metrics functions and domains and includes weaknesses related to the Agency's open prior-year recommendations (refer to **Appendix III**) and weaknesses from relevant FHFA-OIG audits that impact the IG FISMA Reporting Metrics. The weaknesses from the relevant FHFA-OIG audits are included in this report by reference only.

In combination, these control weaknesses affect the Agency's ability to preserve the confidentiality, integrity, and availability of its information and information systems, potentially exposing it to unauthorized access, use, disclosure, modification, or destruction. These key weaknesses need to be addressed in a comprehensive manner to achieve an effective rating of Level 4 – *Managed and Measurable*.

Table 2: Weaknesses Noted in FISMA Audit Mapped to the CSF Functions and Domains in the IG FISMA Reporting Metrics

CSF Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
Govern	Cybersecurity Governance	FHFA did not conduct and document annual security control assessments (**Finding 1**). FHFA-OIG audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025* (July 30, 2025) (AUD-2025-004), had an open prior-year recommendation related to performing CSF activities.
	Cybersecurity Supply Chain Risk Management	No weaknesses identified.
Identify	Risk and Asset Management	FHFA did not conduct and document annual security control assessments (**Finding 1**). FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to software management controls. FHFA-OIG's ongoing FY 2026 internal penetration test of FHFA's network and systems revealed Office of the Chief Information Officer's (OCIO) shortcomings for this domain.
Protect	Configuration Management	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023) (AUD-2023-004), had an open prior-year recommendation related to remediating vulnerabilities in a timely manner. FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to vulnerability management controls. FHFA-OIG's ongoing FY 2026 internal penetration test of FHFA's network and systems revealed OCIO's shortcomings for this domain.
	Identity and Access Management	FHFA did not disable inactive privileged user accounts for a cloud system in a timely manner and the cloud system's user re-authorization review did not identify inactive accounts. (**Finding 2**).

CSF Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
		FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020* (October 20, 2020) (AUD-2021-001), had an open prior-year recommendation related to implementing planned multi-factor authentication for privileged accounts for internal systems. FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to access controls. FHFA-OIG's audit report, *Vulnerabilities in FHFA's Public Facing Systems Risk Unauthorized Access to Non-Public Data* (September 25, 2025) (AUD-2025-007), revealed shortcomings related to access controls. FHFA-OIG's ongoing FY 2026 internal penetration test of FHFA's network and systems revealed OCIO's shortcomings for this domain.
	Data Protection and Privacy	FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to data protection and privacy controls. FHFA-OIG's audit report, *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement,* (September 25, 2024) (AUD-2024-010), revealed shortcomings related to data protection and privacy controls.
	Security Training	No weaknesses noted.
Detect	Information Security Continuous Monitoring	FHFA did not conduct and document annual security control assessments (**Finding 1**). FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to Information Security Continuous Monitoring. FHFA-OIG's ongoing FY 2026 internal penetration test of FHFA's network and systems revealed OCIO's shortcomings for this domain.
Respond	Incident Response	FHFA-OIG's audit report, *Vulnerabilities in FHFA's Public Facing Systems Risk Unauthorized Access to Non-Public Data* (September 25, 2025) (AUD-2025-007), revealed shortcomings related to logging and alerting. FHFA-OIG's ongoing FY 2026 internal penetration test of FHFA's network and systems revealed OCIO's shortcomings for this domain.
Recover	Contingency Planning	FHFA-OIG audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025* (July 30, 2025) (AUD-2025-004), had open prior-year recommendations related to performing functional contingency plan tests.

CSF Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
		FHFA-OIG's audit report, *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement,* (September 25, 2024) (AUD-2024-010), revealed shortcomings related to contingency planning.

Source: Sikich's analysis of the Agency's weaknesses identified during this year's FISMA audit, open prior-year recommendations, and relevant FHFA-OIG audits, mapped back to the IG FISMA Reporting Metrics.

The following section provides a detailed discussion of the audit findings. **Appendix I** provides background information on FISMA. **Appendix II** describes the audit objectives, scope, and methodology. **Appendix III** provides the status of prior-year recommendations. **Appendix IV** includes the Agency's comments.

3.0 Audit Findings

1. FHFA Did Not Conduct and Document Annual Security Control Assessments.

CSF Functions: *Govern, Identify, and Detect*

IG FISMA Reporting Metrics Domains: *Cybersecurity Governance, Risk and Asset Management, and Information Security Continuous Monitoring*

We found that FHFA did not conduct annual security control assessments and develop assessment reports documenting the results for three of the four systems selected for testing. Additionally, FHFA did not establish Plans of Action and Milestones (POA&Ms) to address the lack of annual security control assessments. Specifically, we found that the following systems had outdated security control assessments:

- General Support System (GSS)[12] – last control assessment report dated August 27, 2024.
- A Security Information and Event Management (SIEM) application[13] – last control assessment report dated March 20, 2025.
- Suspended Counterparty System (SCP)[14] – last control assessment report dated February 24, 2025.

FHFA officials explained that annual security control assessments did not follow the standard predetermined cycle because Authority to Operate (ATO) extensions were documented with an expiration date of October 15, 2027, to allow time to support FHFA's on-going security authorizations transformation[15] of these systems. The same FHFA officials further noted that after the completion of full system reassessments, FHFA will revert back to the standard cycle of annual security control assessments. Specifically, the *ATO Extension and Phased Reauthorization of FHFA Information Systems Memorandum* (September 11, 2025), states the following:

> *To ensure mission continuity while aligning with federal security requirements, this memorandum establishes a structured approach allowing continued system operation during a fixed ATO period while systems transition through reassessment and reauthorization.*

[12] The FHFA GSS is considered a Wide Area Network and consists of the backbone, a Metropolitan Area Network, and the Local Area Networks at various sites. The GSS provides connectivity between the agency's sites, Headquarters, and Datacenters.

[13] A cloud based SIEM solution used by FHFA OCIO's Operations and Security.

[14] SCP is a system used for tracking suspended counterparty cases.

[15] According to the ATO extensions, during the transformation, the security documentation for these systems will be comprehensively updated, followed by a cyber reassessment to ensure compliance with Federal Information Processing Standards 199 standards. Activities will include a security categorization re-evaluation, transitioning documentation to standardized and modern templates, system re-assessment, security scans, and/or penetration testing, and updating the continuous monitoring plan.

The agency has undergone a significant transformation in recent years, including a shift in personnel and institutional knowledge. Many individuals with historical knowledge of system development and operations are no longer with the agency, while new personnel are in the process of gaining a full understanding of system functionality, dependencies, and associated risks. This transition has highlighted the need for a deliberate and structured approach to ensure system knowledge is retained, risks are effectively managed, and controls remain properly implemented.

In addition, the same FHFA officials stated that the FHFA OCIO did not conduct the annual security control assessments and develop control assessment reports since they were focused on strengthening existing safeguards while maintaining a consistent and acceptable level of risk, rather than conducting and documenting duplicative reassessments of controls already scheduled for redesign or reevaluation.

Furthermore, according to FHFA officials, FHFA did not believe they needed to establish POA&Ms for the lack of annual security control assessments because an *ATO Extension and Phased Reauthorization of FHFA Information Systems Memorandum,* was signed by the Chief Information Officer (CIO) granting continued operation under a fixed ATO period while undergoing reassessment, continuous monitoring, and re-authorization activities.

OMB Circular A-130, *Managing Information as a Strategic Resource (*July 28, 2016), Appendix I, Section 5, subsection e. Security and Privacy Assessments*,* states that, "Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually."

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020 (includes updates as of December 10, 2020)),[16] specifies the following regarding control assessment and POA&Ms:

- Assessment, Authorization, and Monitoring (CA-2), *Control Assessments*, requires that organizations assess the controls in the system and its environment of operation on an organizationally defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and that a control assessment report is produced that documents the results of the assessment.
- Assessment, Authorization, and Monitoring (CA-5), *Plan of Actions and Milestones*, requires that organizations develop POA&Ms for the system to document planned remediation actions to correct weaknesses or deficiencies noted during the assessment of controls. POA&Ms are to be updated based on the findings from controls assessments, and continuous monitoring activities.

The *Federal Housing Finance Agency Common Control Plan* (November 12, 2025), control CA-2, *Control Assessments*, states that FHFA conducts security control assessments on an annual basis for all FHFA FISMA reportable information systems; and that an assessment report is developed at the conclusion of the control assessment. In addition, control CA-5, *Plan of Actions and Milestones*, states that FHFA's POA&Ms may result from deficiencies and failures

[16] On August 27, 2025, NIST issued a minor release of SP 800-53 (Release 5.2.0). Please find the minor release here.

of system security controls discovered during assessment and authorizations, continuous monitoring, and/or other security controls assessment activities.

The absence of annual security control assessments and documented assessment results may limit FHFA's visibility into whether security controls are operating effectively. Although systems were permitted to operate under ATO extensions, the lack of documented assessment results, and POA&Ms may reduce FHFA's ability to identify, track, and remediate control deficiencies in a timely manner. Consequently, FHFA systems could be compromised through unvalidated security weaknesses that remained undetected due to the absence of security assessments and remediation tracking.

We recommend the FHFA Acting Chief Information Officer:

- **Recommendation 1:** Conduct security control assessments on an annual basis and develop assessment reports at the conclusion of the control assessments in accordance with OMB Circular A-130 for the FHFA GSS, SIEM application, and SCP systems.
- **Recommendation 2:** Develop and maintain POA&Ms to track the completion of overdue security control assessments, development of assessment reports, and remediation of deficiencies through assessments for the FHFA GSS, SIEM application, and SCP systems.

2. FHFA Did Not Disable Inactive Privileged User Accounts for a Cloud System in a Timely Manner, and the Cloud System's User Re-authorization Review Did Not Identify Inactive Accounts.

CSF Functions: *Protect*

IG FISMA Reporting Metrics Domains: Identity and Access Management

FHFA did not disable a cloud system's[17] privileged user accounts[18] within 35 days of inactivity. In addition, the cloud system's annual user re-authorization review did not identify inactive or unused privileged user accounts or determine whether users still needed access.

Based on our review of a listing of FHFA's cloud system's privileged user accounts that were active and showed last login date as of November 25, 2025, we found that:

- 5 of 12 enabled privileged user accounts (approximately 42 percent) were not disabled after 35 days of inactivity or had no recorded login activity within the cloud system.

[17] A cloud-based workflow automation platform for managing tasks, activities, and processes through managed workflows.

[18] A privileged system user has elevated application-specific privileges/permissions compared to that of a general system user.

- Two accounts remained enabled beyond 35 days after their last application login and were disabled by an Administrator tool[19] between 37 and 51 days of inactivity by the cloud system.
- Three accounts had no recorded login activity within the cloud system and were disabled between 73 and 538 days of inactivity within the cloud system.

In addition, the annual cloud system's user re-authorization review did not identify these inactive or unused accounts. Specifically, we found that:

- The cloud system's System Owner reauthorized all five users in August 2025.
- The review did not identify that these users did not need continued access or that their access could be reduced.

According to an FHFA official, the 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, under FHFA's current design and implementation of this control, privileged user accounts within the cloud application could remain enabled as long as the associated enterprise directory services account was active, regardless of whether the privileged users had logged into the application or used their privileged access.

In addition, according to an FHFA official, the cloud system's re-authorization review did not include an evaluation of privileged user last login activity for the application.

NIST SP 800-53, Revision 5, requires the following regarding disabling accounts and reviewing user privileges:

- Access Controls (AC-2(3)), *Account Management* | *Disable Accounts,* requires that FHFA disables accounts within an organizationally-defined time period when the accounts have been inactive for an organizationally-defined time period.
- Access Controls (AC-6(7)), *Least Privilege* | *Review of User Privileges,* requires that organizations review privileges assigned to organizationally defined users to validate the need for such privileges, and reassigns or remove privileges if necessary.

In addition, *FHFA Access Control Standard* (October 6, 2025), requires that privileged accounts are disabled after 35 days of inactivity.

Further, FHFA's SSP for the cloud system (September 23, 2025), control, AC-6(7), *Least Privilege* | *Review of User Privileges,* states that the cloud system privileged users are reviewed at least annually by the System Owner. The review is documented using the FHFA User Re-Authorization form. The user review determines if all users still need access or if any accounts or permission levels can be reduced in accordance with the principle of least privilege.

[19] The Administrator tool is an integrated enterprise directory services management and security solution designed to enhance native tools by providing a centralized console for administration, auditing, recovery and delegation. It helps organizations reduce administrative overhead, manage Group Policies, and monitor enterprise directory services health.

Inactive or unused privileged user accounts could remain enabled longer than intended, increasing the risk of unauthorized or inappropriate privileged access to the cloud application, including the cloud system's modules (i.e., Hardware Asset Management or Software Asset Management), as well as unauthorized changes to the cloud system's workflows.

In addition, an ineffective review of the cloud system's privileged user accounts could increase the risk that users retain excessive access privileges beyond their required business need, weakening least privilege enforcement and increasing the risk of unauthorized or unintentional disclosure of sensitive information contained within the cloud system's workflows and modules.

We recommend the FHFA Acting Chief Information Officer:

- **Recommendation 3:** Update the design of the cloud system's privileged account management controls and implement mechanisms to identify and disable inactive privileged user accounts after 35 days of inactivity, based on application-level activity, including accounts that have never logged in.
- **Recommendation 4:** Enhance the cloud system's re-authorization review to include evaluation of privileged user last login activity and validation of continued need for access and appropriate privilege levels, and perform the next review using the updated process.

4.0 Evaluation of Management Comments

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, FHFA management provided their management response related to their specific program findings and recommendations. FHFA management disagreed with the four recommendations in this report. FHFA-OIG management provided their separate management response related to their specific program. **Appendix IV** includes the Agency's comments.

FHFA Response

FHFA Comments to Recommendation 1

FHFA management disagreed with this recommendation and noted that while control assessment reports were not produced in the format expected by the auditors, FHFA, in alignment with OMB Circular A-130, NIST SP 800-37, NIST SP 800-53, and the Agency's continuous monitoring strategy, maintained ongoing visibility into system security posture through a mature continuous monitoring program and operational security oversight activities conducted across the Agency. FHFA management also stated that FHFA continuously evaluates the effectiveness of security controls through recurring managerial, operational, and technical activities. These activities are documented in various reporting formats and consolidated into an annual continuous monitoring report, which enables ongoing assessment and validation of security controls to identify, prioritize, track, and remediate security risks in a timely manner.

FHFA management also acknowledged that it is undergoing a FISMA & Risk Management Framework (RMF) modernization initiative to enhance its enterprise-wide assessment standardization, formalize its assessment reporting, improve evidence management, and strengthen its authorization processes to further mature and streamline RMF execution across all systems.

Response to FHFA Comments to Recommendation 1: As we showed in this report, FHFA management did not provide evidence that annual security control assessments were performed and documented as required by its own policies and procedures, OMB Circular A-130, and NIST SP 800-53. OMB Circular A-130 establishes a continuous, risk-based approach to information security that is implemented through NIST standards and guidelines. Consistent with this framework, NIST SP 800-53, Revision 5, control CA-2, requires organizations to assess security controls at an organization-defined frequency to determine whether controls are implemented correctly, operating as intended, and producing the desired outcome, and to produce a security control assessment report documenting the assessment results. Therefore, FHFA's written response stating that control assessment reports were not produced in the format expected by the auditors is incorrect since no evidence was provided of current security control assessments for 3 of the 4 systems selected for testing.

In addition, while FHFA management stated that continuous monitoring activities were performed and systems operated under approved ATO extensions during reassessment and re-authorization efforts, neither continuous monitoring nor an ATO extension substitutes for an independent assessment of control effectiveness. NIST SP 800-37 identifies ongoing control assessments as a component of an organization's continuous monitoring strategy and notes

that assessment results used to satisfy annual assessment requirements should be current, relevant, and obtained by assessors with the required degree of independence. An expected output for ongoing monitoring includes updated security and privacy assessment reports. Therefore, continuous monitoring provides ongoing visibility into security posture and control effectiveness, but it does not eliminate the requirement to independently assess and document control effectiveness. Although management may have performed monitoring and risk analysis activities, FHFA did not demonstrate that annual security control assessments were completed and documented.

After considering management's response, our recommendation still stands. We encourage FHFA to conduct security control assessments on an annual basis and document assessment reports at the conclusion of the control assessments.

FHFA Comments to Recommendation 2

FHFA management disagreed with this recommendation noting that POA&Ms should not be created solely because standalone annual security control assessment reports were not completed in the format expected by the auditor. Management further stated that since POA&Ms are intended to document and track identified security weaknesses, as well as risks requiring corrective action, FHFA did not believe the absence of an assessment report constitutes evidence of security weaknesses requiring POA&M tracking.

In addition, FHFA management stated that it has completed and documented its security assessments in a consolidated Information System Continuous Monitoring (ISCM) report, and the existence of this report refutes the contention that there is a security weakness requiring POA&M tracking. Further, FHFA management stated that it is improving its RMF processes to enhance evidence management and control assessment templates. FHFA management also stated that it may separately track modernization milestones, assessment documentation improvements, evidence crosswalks, and authorization of artifacts through appropriate program governance mechanisms.

Response to FHFA Comments to Recommendation 2: As we showed in this report, FHFA did not establish POA&Ms to address the lack of annual security control assessments. Specifically, the ISCM report, referenced in FHFA management's written response, states that control assessments for several systems were still in process and those systems have been given ATO extensions. In addition, the ISCM report does not replace the requirement for documenting POA&Ms for lack of security control assessments for these systems. NIST SP 800-53, control CA-5, *Plan of Actions and Milestones*, requires that organizations develop POA&Ms to document planned remediation actions to correct weaknesses or deficiencies.

After considering management's response, our recommendation still stands. We encourage FHFA to develop POA&Ms to track the completion of security control assessments, and the development of assessment reports for the GSS, SIEM application, and SCP systems.

FHFA Comments to Recommendation 3

FHFA management disagreed with this recommendation noting that the recommendation relies exclusively on application-level activity to determine inactivity for privileged accounts. FHFA management further stated that privileged accounts for the cloud system are authenticated through single sign-on (SSO), where a single privileged identity may be authorized to administer multiple enterprise systems. FHFA management also stated that the cloud system implements application-specific authorization controls that govern access independently of enterprise authentication and that its implementation satisfies the intent of its account management policy through a layered approach.

Response to FHFA Comments to Recommendation 3: As we showed in this report, under FHFA's current design, privileged cloud application user accounts remained enabled as long as the associated enterprise directory services account was active, regardless of whether the privileged users had logged into the application or regularly used their privileged access. Specifically, FHFA utilizes SSO on the cloud system using enterprise directory services; however, this does not prevent FHFA from implementing mechanisms to identify and disable privileged accounts after 35 days of application-level inactivity, including accounts that have never logged in.

In addition, the *FHFA Access Control Standard* requires that privileged accounts are disabled after 35 days of inactivity; the standard does not exclude the application layer of systems. As indicated by FHFA's written response, even if a privileged user has not accessed the cloud application over an extended period of time, the privileged account may stay active, as long as they remain active in enterprise directory services.

After considering management's response, our recommendation still stands. We encourage FHFA to update the design of the cloud system's privileged account management controls and implement mechanisms to identify and disable inactive privileged user accounts after 35 days of inactivity, based on application-level activity, including accounts that have never logged in.

FHFA Comments to Recommendation 4

FHFA management disagreed with this recommendation and stated that application-level last-login data may be reviewed as supplemental information, but it is not a determinative factor for privileged access removal. In addition, FHFA management noted that limited or no application login activity does not necessarily indicate that a user lacks a business need for access, as some privileged users may support functions that do not require frequent interactive logins. Further, FHFA management stated that the privileged access re-authorization process is aligned with NIST SP 800-53, AC-2 and AC-6 controls, which emphasize continued business need and least privilege validation.

Response to FHFA Comments to Recommendation 4: As we showed in this report, the annual cloud system's re-authorization review did not identify the inactive and unused accounts identified during the audit. Therefore, the re-authorization review did not identify whether these users required continued access or if their access could be reduced.

In addition, the SSP for the cloud system, control AC-6(7), *Least Privilege* | *Review of User Privileges,* requires that the cloud system's privileged users are reviewed at least annually, and that the review determines if all users still need access or if any accounts or permission levels

can be reduced in accordance with the principle of least privilege. Specifically, as identified during this audit, the annual re-authorization review was not being performed as intended; as privileged users that had not logged on to the cloud system for an extended period of time continued to retain access to the system. Further, these inactive privileged users were not detected through a preventative control (disabling users after a period of inactivity) or a detective control (periodic user access reviews) during that time.

After considering management's response, our recommendation still stands. We encourage FHFA to enhance the cloud system's re-authorization review to include evaluation of privileged user last login activity and validation of continued need for access and appropriate privilege levels, and perform the next review using the updated process.

FHFA-OIG Response

FHFA-OIG did not have any findings and recommendations identified in this report. FHFA-OIG management thanked Sikich for the opportunity to respond to the report.

Appendix I: Background

Federal Information Security Modernization Act of 2014

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads[20] to, among other things:

- Be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; comply with applicable governmental requirements and standards; and ensure information security management processes are integrated with the agency's strategic, operational, and budget planning processes.
- Ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.
- Delegate to the agency's Chief Information Officer the authority to ensure compliance with FISMA.
- Ensure that the agency has trained personnel sufficient to assist the agency in complying with FISMA requirements and related policies, procedures, standards, and guidelines.
- Ensure that the Chief Information Officer reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.
- Ensure that senior agency officials carry out information security responsibilities.
- Ensure that all personnel are held accountable for complying with the agency-wide information security program.

Agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security programs and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agencies' information security programs and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include minimum security requirements and best practices to protect federal systems. In addition, NIST develops and issues the Federal Information Processing Standards and also publishes SPs as recommendations and guidance documents.

[20] 44 U.S. Code (USC) § 3554, *Federal agency responsibilities*.

FISMA Reporting Requirements

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* which provides reporting guidance for FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. As a result, OMB, the CIGIE, and other stakeholders collaborate to develop these metrics.

On March 17, 2026, OMB and CIGIE issued a joint communication noting that in order to meet the FISMA independent evaluation requirements, IG's and independent external auditors are directed to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits. Therefore, we performed the audit using the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* and the FY 2025 IG FISMA Reporting Metrics.

As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and practices alignment with the six functional areas in the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 3: Alignment of the CSF Functions to the Domains in the IG FISMA Reporting Metrics

CSF Function	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	**Cybersecurity Governance and Cybersecurity Supply Chain Risk Management**
Identify	The organization's current cybersecurity risks are understood.	**Risk and Asset Management**
Protect	Safeguards to manage the organization's cybersecurity risks are used.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	**Information Security Continuous Monitoring**
Respond	Actions regarding a detected cybersecurity incident are taken.	**Incident Response**
Recover	Assets and operations affected by a cybersecurity incident are restored.	**Contingency Planning**

Source: Sikich's analysis of the NIST CSF 2.0 and the FY 2025 IG FISMA Reporting Metrics

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of at least Level 4: *Managed and Measurable.*

Table 4: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess the policies and procedures and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2025 IG FISMA Reporting Metrics

Appendix II: Objective, Scope, and Methodology

FHFA-OIG engaged Sikich to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of the Agency's information security programs and practices.

Objective

The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (IG FISMA Reporting Metrics).

Scope

The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2025, through March 31, 2026. Within this period, we assessed the Agency's information security programs and practices' consistency with FISMA and reporting instructions issued by OMB and DHS for FY 2026. The scope of the audit also included assessing selected controls from NIST SP 800-53, Revision 5, supporting the IG FISMA Reporting Metrics, for a sample of 4 systems from the 47 systems in FHFA's FISMA inventory of information systems and a sample of 2 systems from the total population of 23 FHFA-OIG FISMA information systems (**Table 5**).

Table 5: Description of Systems Selected for Testing

Entity	System	Description
FHFA	GSS	The FHFA GSS is considered a Wide Area Network and consists of the backbone, a Metropolitan Area Network, and the Local Area Networks at various sites. The GSS provides connectivity between the agency's sites, Headquarters, and Datacenters.
FHFA	Cloud System	A cloud-based workflow automation platform for managing tasks, activities, and processes through managed workflows.
FHFA	SIEM System	A SIEM solution used by FHFA OCIO Operations and Security.
FHFA	SCP	SCP is a system used for tracking suspended counterparty cases.
FHFA-OIG	OIGNet GSS	The FHFA-OIG GSS is a general purpose, multi-user system used throughout FHFA-OIG. Its users are primarily composed of those with desktops and laptops and other ancillary equipment connected to FHFA-OIG network and central servers that support FHFA-OIG. The core network infrastructure consists of network switches, firewalls, and routers that provide boundary protection and network segmentation.
FHFA-OIG	Cloud System	A cloud-based system used to store, share, and collaborate on documents.

Source: Sikich's analysis of the system descriptions in the system inventories and applicable SSPs.

For this year's review, IGs were to assess 20 core and 5 supplemental IG FISMA Reporting Metrics across six function areas — Govern, Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — *Ad-Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.*

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2026 FISMA audits. As part of this approach, core and supplemental IG FISMA Reporting Metrics were averaged independently to determine a domain's maturity level and provide data points for the assessed program and function effectiveness. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to Administration priorities and other high-risk areas. It was recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of overall program and function-level effectiveness.

We used the IG FISMA Reporting Metrics guidance[21] to form our conclusions for each CSF function, domain, and the overall agency rating. Specifically, we focused on the calculated average of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the supplemental IG FISMA Reporting Metrics, progress made in addressing outstanding prior-year recommendations, and other data sources (e.g., relevant FHFA-OIG audits), to form our risk-based conclusion. For the purposes of this audit, we evaluated each metric for FHFA and FHFA-OIG. Where the metric evaluation results differed, we used a risk-based approach to determine the overall maturity of the metric.

The audit also included an evaluation of whether the Agency took corrective action to address open recommendations from the FY 2020 FISMA audit,[22] FY 2023 FISMA audit,[23] FY 2024 FISMA audit,[24] 2025 FISMA audit,[25] and 2025 Privacy audit.[26]

---

[21] The IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on their evaluations. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity lower than Level 4.

[22] FHFA-OIG Audit Report AUD-2021-001, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020* (October 20, 2020).

[23] FHFA-OIG Audit Report AUD-2023-004, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023).

[24] FHFA-OIG Audit Report AUD-2024-006, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024* (July 30, 2024).

[25] FHFA-OIG Audit Report AUD-2025-004, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025* (July 30, 2025).

[26] FHFA-OIG Audit Report AUD-2025-006, *Audit of the Federal Housing Finance Agency's Privacy and Data Protection Program Fiscal Year 2025* (August 27, 2025).

Additionally, Sikich took the following audits into consideration to inform the FISMA audit:

- FHFA-OIG audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007).[27]
- FHFA-OIG audit report, *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement* (September 25, 2024) (AUD-2024-010).[28]
- FHFA-OIG audit report, AUD-2025-007, *Vulnerabilities in FHFA's Public Facing Systems Risk Unauthorized Access to Non-Public Data* (September 25, 2025).[29]

In addition, we consulted with FHFA-OIG regarding its ongoing internal penetration test of FHFA's network and systems that may impact the 2026 FISMA audit.

We conducted audit fieldwork remotely and onsite at the Agency's headquarters in Washington DC, from October 2025 through June 2026.

Methodology

We conducted this performance audit 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.

To determine if the Agency's information security programs and practices were effective, Sikich conducted interviews with Agency officials and reviewed legal and regulatory requirements stipulated in FISMA. Sikich also reviewed documents supporting the information security programs. These documents included, but were not limited to, the Agency's (1) information security policies and procedures, (2) incident response policies and procedures, (3) access control procedures, (4) patch management procedures, (5) change control documentation, and (6) system-generated account listings. Where appropriate, Sikich compared documents, such as information technology policies and procedures, to requirements stipulated in relevant OMB memoranda and NIST SPs. In addition, Sikich performed tests of system processes to determine the adequacy and effectiveness of those controls. In addition, Sikich reviewed the status of FISMA and privacy audit recommendations from FY 2020 through 2025. See **Appendix III** for the status of prior-year recommendations.

In addition, our work in support of the audit was guided by applicable Agency policies and federal guidelines and standards, including, but not limited to, the following:

- *Government Auditing Standards 2024 Revision* (February 2024).
- Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book) (May 2025).

[27] The report can be found here.

[28] The report can be found here.

[29] The report can be found here.

- OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (January 15, 2025).
- *FY 2025 IG FISMA Reporting Metrics v2.0* (April 3, 2025).
- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy* (December 2018).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020 (includes updates as of December 10, 2020)).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- Agency policies and procedures, including but not limited to:
  - *FHFA Access Control Standard* (October 6, 2025).
  - *FHFA Assessment and Authorization Plan* (September 30, 2025).
  - *FHFA Common Control Plan* (November 12, 2025).
  - FHFA's SSP for a cloud system (September 23, 2025).

Sikich judgmentally selected 4 FHFA information systems from the total population of 47 systems in FHFA's FISMA inventory of information systems for testing. The four systems were judgmentally selected based on risk. Specifically, four moderate categorized systems were selected, one being the FHFA GSS that supports FHFA's applications that reside on the network and the other three being systems that had not been tested in prior years.

Additionally, Sikich judgmentally selected 2 information systems from the total population of 23 FHFA-OIG FISMA information systems for testing. The OIGNet was selected based on risk because it is a moderate categorized system that supports FHFA-OIG applications that reside on the network. A cloud system was selected because the system had not been tested in prior FISMA audits. Sikich tested the six systems' selected security controls to support its response to the IG FISMA Reporting Metrics.

We assessed internal controls that we deemed to be significant to the audit objectives. Specifically, we assessed 3 of the 17 principles associated with the 5 components of internal control defined in the GAO's *Standards for Internal Controls in the Federal Government* (May 2025) (the Green Book). The table below summarizes the principles we assessed:

Table 6: GAO Green Book Assessed Principles

Control Activities
Principle 10: Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.
Principle 11: Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.
Principle 12: Management should implement control activities through policies and procedures.

Appendix III: Status of Prior Recommendations

The table below summarizes the status of our follow-up related to the status of the open prior recommendations from the FY 2020 FISMA audit (AUD-2021-001), the FY 2023 FISMA audit (AUD-2023-004), the FY 2024 FISMA audit (AUD-2024-006), the 2025 FISMA audit (AUD-2025-004), and the 2025 Privacy audit (AUD-2025-006).[30]

Report # Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
AUD-2021-001, Finding #3	We recommend that FHFA management: 3. Implement the planned multi-factor authentication for privileged accounts for internal systems (e.g., infrastructure).	We found that the prior-year recommendation has not been completed and remediation was in progress. Management provided an estimated completion date of July 30, 2026.	**Open**
AUD-2023-004, Finding #1	We recommend that FHFA's Acting Chief Information Officer: 2. If FHFA is unable to meet the requirements in OMB M-22-18 and/or OMB M-23-16 in a timely manner, we recommend that the FHFA Chief Information Officer should consider request for an extension or waiver in accordance with OMB M-22-18 and/or OMB M-23-16. If FHFA requests a waiver, FHFA should consider documenting a risk-based decision and document any compensating controls.	We found that the prior-year recommendation has been completed. On January 23, 2026, OMB issued Memorandum M-26-05, *Adopting a Risk-Based Approach to Software and Hardware Security* that rescinded OMB Memoranda M-22-18 and M-23-16 and eliminated the Federal agency requirement to obtain and validate software producer attestations. With the recission of the OMB requirements, FHFA determined further action is not needed to address the recommendation and will continue (as applicable) to document risk-based decisions within its existing governance and Risk Management Framework processes.	**Closed**
AUD-2023-004, Finding #3	We recommend that FHFA's Acting Chief Information Officer:	We found that the prior-year recommendation has not been completed and remediation was in progress. Management provided an estimated completion date of July 30, 2026.	**Open**

[30] See Footnotes 22, 23, 24, 25, and 26.

Report # Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	3. Remediate past due exploitable vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency's (CISA)'s Binding Operational Directive (BOD) 22-01 and the OTIM Vulnerability Management Process.	Based on our analysis of FHFA's vulnerability reports generated from its enterprise vulnerability scanning tool from February 4, 2026, through February 10, 2026, we found 45 vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) catalog that were not remediated within required timeframes.	
AUD-2024-006, Finding #1	We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations: 1. Develop and implement policies and procedures to oversee FHFA's background reinvestigation process, including oversight controls over FHFA's service provider.	We found that the prior-year recommendation has been completed. FHFA developed and implemented policies and procedures to oversee FHFA's background reinvestigation process, including oversight controls over FHFA's service provider.	**Closed**
AUD-2024-006, Finding #1	We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations: 3. Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA and Office of Personnel Management (OPM) standards.	We found that the prior-year recommendation has been completed. FHFA implemented a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA and OPM standards.	**Closed**
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources: 6. Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA-OIG and OPM standards.	We found that the prior-year recommendation has been completed. FHFA-OIG has established a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA-OIG and OPM standards.	**Closed**
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources:	We found that the prior-year recommendation has been completed. FHFA-OIG has established and implemented a process to make suitability adjudicative determinations.	**Closed**

Report # Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	7. Establish and implement a process to make suitability adjudicative determinations and take suitability actions for covered positions in accordance with OPM's regulation under Title 5 Code of Federal Regulations, Part 731.103.		
AUD-2024-006, Finding #4	We recommend that FHFA's Chief Information Officer: 11. Complete the review and update of overdue System Security and Privacy Plans and Customer Control Plans (CCP) in accordance with the existing related POA&Ms.	We found that the prior-year recommendation has been completed. FHFA completed a review and update of overdue SSPs and CCPs.	**Closed**
AUD-2025-004, Finding #1	We recommend the FHFA Chief Information Officer: 1. Establish and implement guidance for performing CSF 2.0 activities through policies and procedures.	We found that the prior-year recommendation has not been completed. FHFA established guidance for performing CSF 2.0 activities by developing the *CSF Implementation Plan*. However, FHFA did not fully implement the CSF activities documented in the implementation plan. The plan details that once FHFA defines current and target profiles, FHFA will analyze and prioritize capability gaps. From this analysis, FHFA develops a prioritized strategy that includes both near-term tactical enhancements and longer-term strategic initiatives. We requested evidence of a gap assessment between current and target profiles and associated action plan, as well as evidence that FHFA periodically monitors and reports on progress in reaching its target profiles. FHFA management noted that they are currently planning these activities.	**Open**
AUD-2025-004, Finding #2	We recommend the FHFA Chief Information Officer: 2. Ensure that Privileged Account Request eWorkflows are fully completed and approved for all privileged FHFA GSS user accounts prior to granting access.	We found that the prior-year recommendation has been completed. FHFA completed and approved Privileged Account Request eWorkflows for FHFA GSS user accounts prior to granting access.	**Closed**

Report # Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
AUD-2025-004, Finding #3	We recommend the FHFA Chief Information Officer: 3. Ensure all applicable Organizational Units (OUs) are included in the automated process that disables inactive accounts after 35 days.	We found that the prior-year recommendation has been completed. FHFA included applicable OUs in the automated process that disables inactive accounts after 35 days.	**Closed**
AUD-2025-004, Finding #3	We recommend the FHFA Chief Information Officer: 4. Disable inactive AD accounts after a period of 35 days of inactivity.	We found that the prior-year recommendation has been completed. FHFA disabled inactive AD accounts after a period of 35 days of inactivity.	**Closed**
AUD-2025-004, Finding #4	We recommend the FHFA Chief Information Officer: 5. Create a POA&M to establish when the annual disaster recovery plan (DRP) exercise will be conducted and when the new system owners will be assigned and trained on their roles and responsibilities related to FHFA GSS, Office of General Counsel (OGC) Matter Management Tracking System, and the Status Tracking and Reporting (STAR) system.	We found that the prior-year recommendation has not been completed. FHFA completed a DRP tabletop exercise for the GSS, OGC Matter Management Tracking System, and the STAR system. However, NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,* requires that a functional exercise at an organization-defined frequency be conducted for moderate-impact systems. Since the FHFA GSS, OGC Matter Management Tracking System, and the STAR system were moderate systems, a functional exercise in accordance with the DRP procedures should be performed.	**Open**
AUD-2025-004, Finding #4	We recommend the FHFA Chief Information Officer: 6. Schedule and conduct an annual DRP exercise for the FHFA GSS, OGC Matter Management Tracking System, and the STAR system, and ensure new system owners are trained to execute them.	We found that the prior-year recommendation has not been completed. FHFA completed a DRP tabletop exercise for the GSS, OGC Matter Management Tracking System, and the STAR system. However, NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,* requires that a functional exercise at an organization-defined frequency be conducted for moderate-impact systems. Since the FHFA GSS, OGC Matter Management Tracking System, and the STAR system were moderate systems, a functional exercise in accordance with the DRP procedures should be performed.	**Open**

Report # Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
AUD-2025-006, Finding #1	We recommend the FHFA Senior Agency Official for Privacy in coordination with the System Owner: 1. Conduct a review of all current privileged user accounts in the FHFA.gov production environment to ensure that each privileged user account has documented access requests and approvals.	We found that the prior-year recommendation has been completed. FHFA completed a review of the active privileged user accounts in the FHFA.gov production environment and verified all assigned roles are authorized.	**Closed**
AUD-2025-006, Finding #1	We recommend the FHFA Senior Agency Official for Privacy in coordination with the System Owner: 2. Update FHFA's *FHFA.gov Customer Controls* to document account management requirements for non-privileged users to include account creation and authorization procedures.	We found that the prior-year recommendation has been completed. FHFA updated the *FHFA.gov Customer Controls* to document account management requirements for non-privileged users to include account creation and authorization procedures.	**Closed**
AUD-2025-006, Finding #2	We recommend the FHFA Senior Agency Official for Privacy in coordination with the System Owner: 3. Evaluate and implement additional FHFA.gov audit logging capabilities to ensure the FHFA.gov audit logs capture access and deactivation events for all user accounts.	We found that the prior-year recommendation has been completed. FHFA evaluated and implemented additional FHFA.gov audit logging capabilities to capture access and deactivation events for user accounts.	**Closed**

Appendix IV: Management's Comments

FHFA's Management Comments

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audit, FHFA-OIG

FROM: Jeffery Harris, Acting Deputy Chief Operating Officer/Chief Information Officer & Chief Information Security Officer, Office of Chief Information Officer /s/

SUBJECT: Management Response for the Draft Report; Performance Audit of FHFA's Information Security Programs and Practices for 2026

DATE: June 30, 2026

This memorandum transmits the management response of the Federal Housing Finance Agency (FHFA), Office of the Chief Information Officer (OCIO), to the FHFA Office of Inspector General (OIG) draft report, "Performance Audit of FHFA's Information Security Programs and Practices for 2026."

Recommendation 1

Conduct security control assessments on an annual basis and develop assessment reports at the conclusion of the control assessments in accordance with OMB Circular A-130 for the FHFA GSS, SIEM application, and SCP systems.

Management Response to Recommendation 1

FHFA disagrees with the OIG recommendation for the following reasons:

- FHFA disagrees with the premise that security control assessment activity was not performed for the GSS, SIEM, and SCP systems. While standalone annual assessment reports were not produced in the format expected by the auditors, FHFA, in alignment with OMB Circular A-130, NIST Special Publications 800-37, 800-53, and the Agency's continuous monitoring strategy, maintained ongoing visibility into system security posture through a mature continuous monitoring program and operational security oversight activities conducted across the Agency. Per these guidance publications, where an organization has implemented a documented continuous monitoring strategy, control assessment activities may be performed through recurring operational, technical, and management activities, as well as in response to specific events.

- Accordingly, FHFA continuously evaluates the effectiveness of security controls through recurring managerial, operational, and technical activities including, but not limited to vulnerability scanning, patch and flaw remediation, audit log monitoring and analysis, incident detection and response, penetration testing, disaster recovery and contingency plan testing, privileged access reviews, updates to System Security Plans (SSPs), and configuration management reviews and associated Security Impact Analyses (SIAs) to determine risk associated with operational or architectural changes. These activities are documented in various reporting formats and consolidated into an annual continuous monitoring report and provide ongoing assessment and validation of security controls and enable FHFA to identify, prioritize, track, and remediate security risks in a timely manner.
- FHFA agrees that continuous and ongoing assessments of controls are important but does not agree that the absence of standalone annual assessment reports alone resulted in an inability to track or remediate deficiencies, as risk tracking and remediation activities were actively occurring through existing cybersecurity governance and operational processes. NIST SP 800-53A provides assessment procedures and supports documenting assessment results but does not independently establish an annual Security Assessment Report (SAR) requirement. Further, NIST SP 800-53 states that "to satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities; Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring during the system life cycle; Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed; After the initial authorizations, organizations assess controls during continuous monitoring."
- Through FHFA's ongoing FISMA & RMF Modernization (FIRM) Initiative, the Agency is implementing enhanced enterprise-wide assessment standardization, formalized assessment reporting, improved evidence management, and strengthened authorization processes to further mature and streamline RMF execution across all systems.
- The systems operated under documented Authority to Operate (ATO) extensions. The extension process was implemented to maintain mission continuity, monitoring, and security analysis while the systems transitioned through reassessment and reauthorization.

Recommendation 2

Develop and maintain POA&Ms to track the completion of overdue security control assessments, development of assessment reports, and remediation of deficiencies through assessments for the FHFA GSS, SIEM application, and SCP systems.

Management Response to Recommendation 2

FHFA disagrees with the OIG recommendation for the following reasons:

- FHFA disagrees that Plans of Actions and Milestones (POA&Ms) should be created solely because standalone annual security control assessment reports were not completed in the format expected by the auditor. A POA&M is intended to document and track identified security weaknesses, as well as risks requiring corrective action. FHFA does not believe

the absence of an assessment report, standing alone, constitutes evidence of a security weakness requiring POA&M tracking.

- FHFA has completed and documented its security assessments in a consolidated Information System Continuous Monitoring (ISCM) report. Existence of this report refutes the contention that there is a security weakness requiring POA&M tracking. Furthermore, the systems listed in the recommendation remained subject to continuous monitoring to include, but not limited to, vulnerability management, flaw remediation, access reviews, change management, incident monitoring, and authorization oversight.
- FHFA believes the issue is more accurately characterized as a documentation format and traceability improvement opportunity, not as an absence of risk management activity or as an unremediated control failure.
- FHFA will continue to use POA&Ms for identified deficiencies, vulnerabilities, audit findings, and risk-based remediation actions. FHFA may separately track modernization milestones, assessment documentation improvements, evidence crosswalks, and authorization of artifact updates through appropriate program governance mechanisms.

Recommendation 3

Update the design of the cloud system's privileged account management controls and implement mechanisms to identify and disable inactive privileged user accounts after 35 days of inactivity, based on application-level activity, including accounts that have never logged in.

Management Response to Recommendation 3

FHFA disagrees with the OIG recommendation for the following reasons:

- FHFA policy requires inactive accounts to be disabled after 35 days of inactivity. However, the recommendation relies exclusively on application-level activity to determine inactivity for privileged accounts, which does not accurately reflect how privileged identities are managed within FHFA's enterprise identity architecture.
- Privileged accounts for the cloud system are authenticated through enterprise directory services and single sign-on (SSO), where a single privileged identity may be authorized to administer multiple enterprise systems and services. As a result, an enterprise-privileged account may remain active through legitimate administrative use across the enterprise, even if the individual cloud application has not been accessed within a 35-day period. Measuring inactivity solely within the application could incorrectly identify valid enterprise-privileged accounts as inactive.
- In addition, the cloud system implements application-specific authorization controls that govern privileged access independently of enterprise authentication. These controls provide an additional layer of access enforcement, ensuring that only authorized users may exercise privileged functions within the application regardless of enterprise authentication status.
- FHFA's implementation satisfies the intent of the Agency's account management policy through a layered identity and access management model that combines enterprise directory services, SSO, privileged access governance, application-level authorization controls, periodic access reviews, and continuous monitoring.

- Management does not concur that disabling privileged accounts based solely on application-level inactivity represents the appropriate control implementation for this environment or that it more effectively achieves the underlying security objective than the existing enterprise approach.

Recommendation 4

Enhance the cloud system's re-authorization review to include evaluation of privileged user last login activity and validation of continued need for access and appropriate privilege levels and perform the next review using the updated process.

Management Response to Recommendation 4

FHFA disagrees with the OIG recommendation for the following reasons:

- FHFA disagrees that the annual re-authorization review was ineffective because it did not use application-level last-login activity as a determinative factor. The purpose of re-authorization is to validate continued business need, assigned role appropriateness, and least-privilege alignment.
- FHFA does not agree that users with limited or no application login activity necessarily lack a business need for access. Some privileged users may support security, administrative, implementation, operational, or contingency functions that do not require frequent interactive logins. Therefore, the absence of recent application-level activity should be reviewed in context rather than treated as automatic evidence that access is no longer required.
- FHFA's privileged access re-authorization process is already aligned with NIST SP 800-53 AC-2 and AC-6 requirements, which emphasize continued business need and least-privilege validation. Application-level last-login data may be reviewed as supplemental information, but it is not a determinative factor required by NIST for privileged access removal.

cc: Abdil Salah
Edom Aweke
Ivan Bengtson
Shelly Blackston

FHFA-OIG's Management Comments

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

June 30, 2026

TO: Sikich CPA LLC

THRU: Brian W. Baker, Deputy Inspector General for Administration /s/

FROM: Michael S. Smith, Chief Information Officer /s/

SUBJECT: Draft Audit Report: Performance Audit of FHFA's Information Security Programs and Practices for 2026

Thank you for the opportunity to respond to Sikich's audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG) information security programs and practices for fiscal year 2026. We trust that the results of this independent audit will provide assurance to our stakeholders that FHFA-OIG's Information Security Program and practices are operating effectively in compliance with FISMA legislation, OMB guidance, and NIST Special Publications. These independent audit results confirm that our Information Technology infrastructure, policies, procedures and practices are suitably designed and implemented to provide reasonable assurance of adequate security.

We appreciate Sikich's professionalism in conducting this year's audit. If you have any questions, please feel free to contact me at 202-730-0401 or michael.smith@fhfaoig.gov.

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219