Federal Housing Finance Agency
Office of Inspector General

# Audit of the Federal Housing Finance Agency's Privacy and Data Protection Program Fiscal Year 2025

Audit Report • AUD-2025-006 • August 27, 2025

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

August 27, 2025

**TO:** Brent Burris, Senior Agency Official for Privacy

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

**SUBJECT**: Audit Report, *Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2025* (AUD-2025-006)

We are pleased to transmit the subject report.

Federal law as directed in 42 United States Code (U.S.C.) § 2000ee-2, *Privacy and Data Protection Policies and Procedures,* requires federal agencies to establish and implement comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form related to employees and the public. Such procedures must be consistent with legal and regulatory guidance, including Office of Management and Budget regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002. Additionally, 42 U.S.C. § 2000ee-2 requires that Inspectors General periodically review their respective agencies' privacy and data protection program.

We contracted with Sikich CPA LLC (herein referred to as "Sikich"), a certified independent public accounting firm, to conduct the fiscal year 2025 independent evaluation of the Agency's (collectively, the Federal Housing Finance Agency (FHFA) and the FHFA Office of Inspector General (OIG)) implementation of privacy and data protection policies and procedures, as directed in 42 U.S.C. § 2000ee-2. Sikich conducted this performance audit under generally accepted government auditing standards. The audit objective was to assess the Agency's implementation of its privacy and data protection program in accordance with federal law, regulation, and policy. Specifically, the audit determined whether the Agency implemented comprehensive privacy and data protection policies and procedures governing the Agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public.

Sikich concluded that, while the Agency generally implemented comprehensive privacy and data protection policies procedures, and practices, its implementation of certain privacy and data protection requirements were not fully achieved. Specifically, Sikich noted weaknesses in access authorizations and approvals, and audit logging capabilities. To address these weaknesses,

Sikich made three recommendations to assist the Agency in strengthening its privacy and data protection program and practices.

Pursuant to 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 privacy and data protection programs and practices in compliance with the Privacy Act of 1974 and related information security policies, procedures, standards, and guidelines. Sikich is responsible for the attached auditor's report dated August 05, 2025, 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.

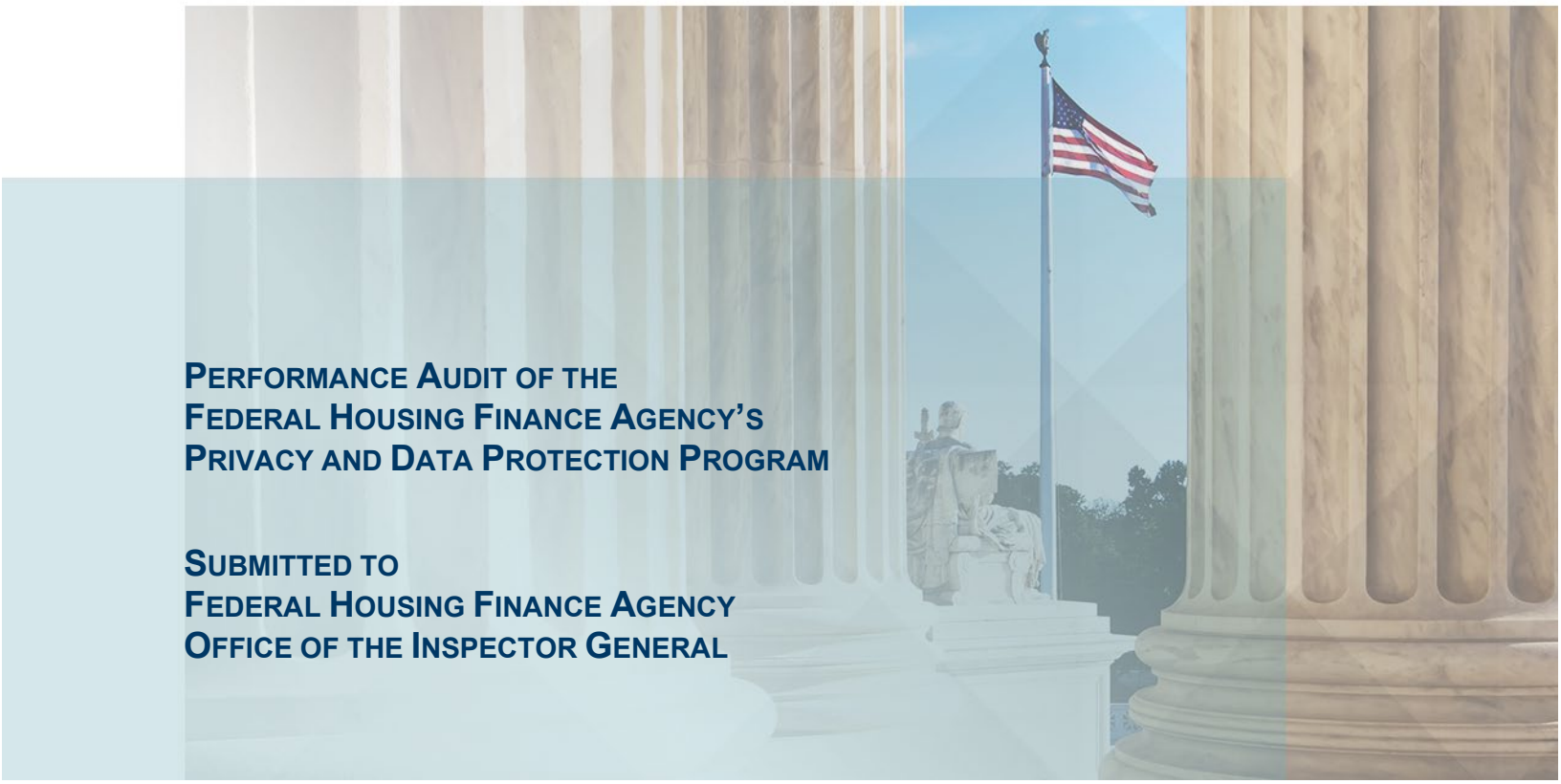
As discussed in the Sikich's report, the Agency's management agreed with the recommendations and outlined its plans to address them.

Attachment

**ATTACHMENT**

Audit of the Federal Housing Finance Agency's
Privacy and Data Protection Program
Fiscal Year 2025

SIKICH®



# PERFORMANCE AUDIT OF THE FEDERAL HOUSING FINANCE AGENCY'S PRIVACY AND DATA PROTECTION PROGRAM

**SUBMITTED TO**
**FEDERAL HOUSING FINANCE AGENCY**
**OFFICE OF THE INSPECTOR GENERAL**

**PERFORMANCE AUDIT REPORT**

**AUGUST 5, 2025**

SIKICH®

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

SIKICH.COM

August 5, 2025

John Allen
Acting Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Acting Inspector General Allen:

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, implementation of privacy and data protection policies and procedures, as directed in 42 United States Code (U.S.C.) § 2000ee-2. We performed this audit under contract with the FHFA-OIG.

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection program in accordance with law, regulation, and policy. Specifically, the audit was designed to determine whether the Agency implemented comprehensive privacy and data protection policies and procedures governing the Agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to Agency employees and the public.

The audit covered the period from April 1, 2023, through March 31, 2025. We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through June 2025.

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 have reviewed the Agency's responses to a draft of this report and have included our evaluation of management's comments within this final report. The Agency's comments are included in **Appendix V**.

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.

*Sikich CPA LLC*

Alexandria, VA

## TABLE OF CONTENTS

## I. EXECUTIVE SUMMARY

Title 42 United States Code (U.S.C.) § 2000ee-2, *Privacy and Data Protection Policies and Procedures*, requires federal agencies to establish and implement comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form related to employees and the public. Such procedures must be consistent with legal and regulatory guidance, including Office of Management and Budget (OMB) regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002. Additionally, 42 U.S.C. § 2000ee-2 requires that Inspectors General periodically review their respective agencies' privacy and data protection program.

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged Sikich CPA LLP (Sikich) to conduct a performance audit to review FHFA's and FHFA-OIG's, collectively referred to as the Agency for reporting combined results, implementation of privacy and data protection policies and procedures, as directed in 42 U.S.C. § 2000ee-2.

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether the Agency implemented comprehensive privacy and data protection policies and procedures governing the Agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public.

In addition, the audit included evaluating whether FHFA took corrective actions to address privacy-related findings and recommendations in FHFA-OIG Audit Report AUD-2023-006*, Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023).[1]

The scope of this performance audit included the Agency's privacy and data protection program and practices covering the period from April 1, 2023, through March 31, 2025.[2] We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through June 2025.

The audit included tests of the Agency's implementation of federal privacy laws, regulations, standards, and its privacy and data protection policies, procedures, and practices. These privacy requirements were mapped to applicable privacy controls outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.[3] The NIST controls catalog provides a consolidated list of privacy control requirements established by the Privacy Act of 1974, Section 208 of the e-Government Act of 2002, and OMB memoranda.

[1] The recommendations from the 2023 Privacy Program audit were evaluated and closed as part of the 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).

[2] The scope of this audit covered the period since the FHFA-OIG Audit Report AUD-2023-006*, Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023).

[3] See Appendix III for mapping of controls.

The audit also included an assessment of the implementation of federal privacy requirements for a judgmental sample of three[4] information systems from the total population of 25 information systems in FHFA's Federal Information Security Modernization Act of 2014 (FISMA)[5] inventory of information systems that required a System of Records Notice (SORN)[6] and a Privacy Impact Assessment (PIA)[7] and one FHFA-OIG[8] information system from the total population of 14 FHFA-OIG FISMA information systems that required a PIA. The one information system selected for FHFA-OIG also required a SORN.

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 concluded that collectively the Agency generally implemented comprehensive privacy and data protection policies, procedures, and practices governing the Agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to agency employees and the public. Specifically, we noted that the Agency had implemented the following privacy and data protection requirements:

- Designating a Senior Agency Official for Privacy (SAOP) (also referred to as Chief Privacy Officer) with responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program.
- Documenting and maintaining current SORNs.
- Reporting annually on the activities of the agency that affect privacy.
- Reviewing and approving the categorization of information systems that collect, house, or utilize personally identifiable information (PII)[9] in accordance with Federal Information Processing Standards.

[4] We sampled the following FHFA systems: Employment Matters Tracking, FHFA.gov, and Financial Disclosure Reporting System. See Appendix II, Table 2 for a description of the systems.

[5] The FISMA Law 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.

[6] A SORN is a notice published in the Federal Register, required by the Privacy Act of 1974, intended to alert the public that a Federal agency has created, modified, or abolished a system of records. A SORN is required when a federal system contains records about an individual that can be retrieved by a unique identifier (e.g., name, social security number).

[7] A PIA is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.

[8] We sampled the following FHFA-OIG system: Office of Investigations Case Management System (OI-CMS). See Appendix II, Table 2 for a description of the system.

[9] PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- Designating which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency; coordinating with agency programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls; and providing oversight of privacy controls.
- Taking steps to limit the collection of PII to what is relevant and necessary.
- Posting privacy policies on agency web sites used by the public.

Although the Agency generally implemented comprehensive privacy and data protection policies procedures, and practices, its implementation of certain privacy and data protection requirements were not fully achieved. In this audit, we noted weaknesses in access authorizations and approvals, and audit logging capabilities (see findings in **Table 1**). In combination, these control weaknesses could affect the Agency's ability to govern the collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to agency employees and the public. As such, we made three recommendations to assist the Agency in strengthening its privacy and data protection program and practices.

In addition, FHFA-OIG's audit report[10] revealed shortcomings related to data loss prevention controls that was considered in our evaluation of the Agency's privacy program. The weaknesses from the FHFA-OIG audits are included in this report by reference only.

**Table 1: Summary of Findings and Recommendations**

| Privacy Program Weaknesses | Recommendations |
|---|---|
| 1. FHFA Did Not Document Formal Approval For User Access to the FHFA.gov System. | **Recommendation 1:** We recommend that FHFA's SAOP in coordination with the System Owner, 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.<br><br>**Recommendation 2:** We recommend that FHFA's SAOP in coordination with the System Owner, update FHFA's *FHFA.gov Customer Controls* to document account management requirements for non-privileged users to include account creation and authorization procedures. |
| 2. FHFA's Audit Logs Did Not Record When Inactive FHFA.gov Accounts were Disabled. | **Recommendation 3:** We recommend that FHFA's SAOP in coordination with the System Owner, evaluate and implement additional FHFA.gov audit logging capabilities to ensure the FHFA.gov audit logs captures access and deactivation events for all user accounts. |

*Source: Sikich's analysis of the Agency's privacy and data protection program and practices.*

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

[10] Recommendations 11, 12, and 13 in 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).

## II. AUDIT FINDINGS

### 1. FHFA Did Not Document Formal Approval for User Access to the FHFA.gov System

The FHFA did not document formal approval for user access to the FHFA.gov system. Specifically, for all 12 sampled new hires (2 privileged[11] and 10 non-privileged[12] users) with access to FHFA.gov,[13] no evidence of documented access approval was provided by FHFA.

For privileged users, FHFA staff referenced electronic mail communications as the basis for access, but no centralized or retrievable record of approval by the designated System Owner or Authorized Approver was available. For non-privileged users, the *FHFA.gov Customer Controls* (March 28, 2025) do not define or document the account management controls related to access authorizations and approvals.

According to an FHFA Office of Congressional Affairs and Communication (OCAC) official,[14] one of the privileged users was given access by email during the system's development and testing phase. Another OCAC official stated that the user, a developer, was authorized for access by an OCAC official who served as both the System Owner and the contract Contracting Officer's Representative, during the development of the system. When the system transitioned to production, FHFA did not formally document or reauthorize that access in accordance with its current access control policies, which is the reason why the user retained the privileged access without recorded approval.

For the second privileged user, the previous System Owner and the backup System Owner confirmed an access request was not received.

For the non-privileged users, access is automatically granted to any FHFA network users that navigates to a designated web page and the user is automatically authenticated using single sign-on. However, the *FHFA.gov Customer Controls* did not document the account management requirements for non-privileged users and how their access would be provisioned.

The *FHFA.gov Customer Controls* (March 28, 2025), security control AC-2 (Account Management), states that, the FHFA System Owner is responsible for approving the creation of any content management account with the Administrator or Content Editor role within any FHFA content management environment. This approval may be granted via email from the System Owner to a content management administrator who will create the account and assign the permissions identified by the System Owner.

[11] These FHFA.gov users have a role of Administrator, which grants full access to all content management settings in the development, test, stage and production environments. The Administrator role is a privileged account with elevated permissions and access rights within the system. FHFA's content management system for the FHFA public website is located within a cloud platform, which provides a secure hosting platform for FHFA to build and manage their content management application environments.

[12] The FHFA.gov non-privileged users have the role of Authenticated User, which is used to preview drafted web pages before they are published.

[13] A random sample of 2 privileged users and 10 non-privileged users with access to FHFA.gov. These users were selected from a population of new hires from April 1, 2023 to December 31, 2024.

[14] OCAC is the FHFA office of the individuals who serve as the FHFA.gov system owner and backup system owner.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), security control Access Control (AC-2) (Account Management), requires organizations to define and document the types of accounts allowed; the authorized users of the system and their access authorizations (i.e., privileges) and intended system usage; and who is authorized to approve access requests.

Failure to document approvals for privileged roles in accordance with FHFA's access control policies may increase the risk that individuals are provided privileged user access rights that is in excess of their role and responsibilities. This could result in unintentional disclosure of sensitive or confidential information, privileged access misuse, and reduced accountability for system changes.

In addition, the lack of formal, documented user account management requirements for non-privileged users could increase the risk that users could be given access to sensitive or confidential data and systems that exceeds their roles and responsibilities. This could result in unintentional disclosure of sensitive or confidential information.

We recommend the FHFA Senior Agency Official for Privacy in coordination with the System Owner:

- **Recommendation 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.
- **Recommendation 2:** Update FHFA's *FHFA.gov Customer Controls* to document account management requirements for non-privileged users to include account creation and authorization procedures.

## 2. FHFA's Audit Logs Did Not Record When Inactive FHFA.gov Accounts Were Disabled

The FHFA audit logs for FHFA.gov did not consistently record the dates and time when FHFA.gov accounts were disabled[15] or blocked.[16] Based on review of the FHFA.gov user listing[17] as of February 7, 2025, there were no audit records to show that 10 of 131 user accounts (approximately 8 percent) were changed to disabled after 90 days of inactivity.[18] Further, there were no audit records to show that four of these user accounts (approximately 3 percent) were changed to blocked after 97 days of inactivity. According to OCAC officials, disabled users may be able to self-reactivate their accounts without assistance, while blocked users must contact an administrator. However, FHFA.gov's audit logs did not consistently record these changes in the users' status, or the actions taken to restore access.

[15] Disabling inactive accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

[16] The same OCAC official stated that a blocked user will get an error message and must contact the system administrator to unblock their account.

[17] FHFA provided a user listing of FHFA.gov account owners. The user listing includes the account owner's username, role, account creation date, and date of last system access.

[18] The same OCAC official stated that a deactivated user is able to self-reactivate their account by going to a designated web page.

An OCAC official stated that FHFA.gov audit logs are incomplete and do not provide a full history of account and system activities. The same official acknowledged that the FHFA.gov audit logs could be improved and that modules[19] could be developed to provide better audit logs.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), security control Audit and Accountability (AU-3) (Content of Audit Records), states the following:

> *Ensure that audit records contain information that establishes the following:*
> *a. What type of event occurred;*
> *b. When the event occurred;*
> *c. Where the event occurred;*
> *d. Source of the event;*
> *e. Outcome of the event; and*
> *f. Identity of any individuals, subjects, or objects/entities associated with the event.*

Further, NIST SP 800-53, Revision 5, security control Access Control (AC-2), enhancement 3 (Account Management, Disable Accounts), requires that organizations disable accounts when the accounts have been inactive for an organizationally defined time period.

*FHFA.gov Customer Controls* (March 28, 2025) states for Auditing and Audit Log Review (AU-2, AU-7) that the content management Events Log Track maintains a database of the last 6-months of auditable events occurring within each content management environment. This includes events related to role or privilege changes, configuration changes, login and logout events as well as public access records. Event Logs are available to the FHFA system owner and developers for troubleshooting or investigative review, to be utilized as needed.

In addition, the *FHFA.gov Customer Controls* states the Deactivate Users module is intended to disable content management accounts for users that have not accessed within 90 days and then to block accounts within 97 days.

Without complete audit logs, FHFA may not be able to determine individual accountability, reconstruct security events, detect intruders attempts to exfiltrate sensitive or confidential data and access systems, or identify system interruptions.

We recommend the FHFA Senior Agency Official for Privacy in coordination with the System Owner:

- **Recommendation 3:** Evaluate and implement additional FHFA.gov audit logging capabilities to ensure the FHFA.gov audit logs captures access and deactivation events for all user accounts.

[19] A content management module is a functional plugin that are either part of the content management core (they ship with content management) or are contributed items that have been created by members of the content management community. Modules build on content management's core functionality, allows the user to customize the data items (fields) on their node types; programmatically sort and display content (custom output controlled by filters defined by the user); and more.

## III. Evaluation of Managements Comments

In response to a draft of this report, FHFA provided a management response related to specific privacy program findings and recommendations. FHFA management fully agreed with the three recommendations in this report, and they outlined their plans to address each recommendation. FHFA-OIG management provided their separate management response related to their specific privacy program. **Appendix V** includes the Agency's comments.

### *FHFA Response*

For Recommendation 1, FHFA management agreed with this recommendation. FHFA management stated that the SAOP has confirmed that the system owner reviewed and verified that all approvals for current privileged user accounts in the FHFA.gov production environment are documented. We consider FHFA's corrective action to meet the intent of our recommendation. Because the remediation occurred after our audit period and is an ongoing process, the remediation of this recommendation will be evaluated in the next Privacy or FISMA audits.

For Recommendation 2, FHFA management agreed with this recommendation. FHFA management stated that individually documented access approvals for non-privileged users (i.e., Authenticated Users) was not and will not be required pursuant to the FHFA.gov Customer Controls document. By September 30, 2025, FHFA will revise the Customer Controls document to clarify that the account creation and authorization process for Authenticated Users is implemented via single sign-on authentication. FHFA's planned corrective action meets the intent of our recommendation.

For Recommendation 3, FHFA management agreed with this recommendation. FHFA management stated that the SAOP has confirmed that the system owner implemented additional logging capabilities to capture access and deactivation events for all user accounts. We consider FHFA's corrective action to meet the intent of our recommendation. Because the remediation occurred after our audit period and is an ongoing process, the remediation of this recommendation will be evaluated in the next Privacy or FISMA audits.

### *FHFA-OIG Response*

FHFA-OIG did not have any findings and recommendations identified in this report. FHFA-OIG management stated that they trust the results of this independent audit will provide assurance to its stakeholders that FHFA-OIG's Privacy Program and practices are operating in accordance with federal law and regulation.

APPENDIX I: BACKGROUND

## Federal Privacy Requirements

The following provides a high-level summary of the relevant federal privacy regulations, standards, and guidance used to guide the performance of this audit.

### The Privacy Act of 1974, 5 U.S.C. Section 552a

The Privacy Act of 1974, 5 U.S.C. Section 552a, as amended, requires agencies to collect only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained and must not disclose this information except under certain circumstances.

Agencies are required to publish a system of records notice to inform the existence of the system and character of the system, such as, describing the routine use of the records contained in the system, including the categories of users and purpose of such use, and the policies and practices of the agency regarding storage, retrievability, access controls, retention and disposal of the records. Further, agencies are to make a reasonable effort to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

### 42 U.S.C. § 2000ee–2, Privacy and Data Protection Policies and Procedures

42 U.S.C. § 2000ee–2, among other things, requires each agency to have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:

1. Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;
2. Assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program;
3. Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974;
4. Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
5. Conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected;
6. Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11 internal controls, and other relevant matters;
7. Ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

8. Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and
9. Ensuring compliance with the Departments established privacy and data protection policies.

**Section 208 of the E-Government Act of 2002**

Section 208, Privacy Provisions, of the E-Government Act of 2002 (Public Law 107-347; 44 U.S.C. 3501 note) requires agencies to 1) conduct PIAs of information technology and collections and, in general, make PIAs publicly available; 2) post privacy policies on agency websites used by the public; and 3) translate privacy policies into a machine-readable format.

**OMB Circular No. A-130, *Managing Information as a Strategic Resource***

OMB Circular No. A-130, Appendix II, Responsibilities for Managing Personally Identifiable Information (July 28, 2016), outlines some of the general responsibilities for federal agencies managing information resources that involve PII and summarizes the key privacy requirements included in other sections of the Circular.

**NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations***

NIST SP 800-53, Revision 5, provides a catalog of security and privacy controls, and is designed to help organizations identify the security and privacy controls needed to manage risk and to satisfy the security and privacy requirements in FISMA, the Privacy Act of 1974, OMB policies and designated Federal Information Processing Standards, among others.

## APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY

FHFA-OIG engaged Sikich to conduct a performance audit in support of the requirement in 42 U.S.C. § 2000ee-2 that Inspectors General periodically review their respective agencies' privacy and data protection program.

### *Objective*

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether the Agency implemented comprehensive privacy and data protection policies and procedures governing the Agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public.

### *Scope*

The scope of this performance audit covered the Agency's privacy and data protection program and practices from April 1, 2023, through March 31, 2025.[20] Within this period, we assessed the Agency's compliance with privacy and data protection requirements in accordance with law, regulation, and policy. The Agency's privacy and data protection program and practices were reviewed within the context of the requirements and recommendations of, but not limited to, 42 U.S.C. § 2000ee-2, the Privacy Act of 1974 Section 552a, as amended; Section 208 of the E-Government Act of 2002; and OMB memoranda.

The audit included tests of the Agency's compliance with federal privacy laws, regulations, standards, and the Agency's privacy and data protection policies, procedures, and practices. These privacy requirements were mapped to applicable privacy controls outlined in NIST SP 800-53, Revision 5.[21] The NIST controls catalog provides a consolidated list of security and privacy control requirements established by the Privacy Act of 1974, Section 208 of the e-Government Act of 2002, 42 U.S.C. § 2000ee-2, and OMB memoranda. We assessed the Agency's performance and compliance in the following areas:

[20] The scope of this audit covered the period since the FHFA-OIG Audit Report AUD-2023-006*, Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023).

[21] Privacy controls are incorporated within NIST SP 800-53, Revision 5, available online here.

- Governance and privacy program
- Inventory of PII
- Privacy impact and risk assessment
- Protection of PII
- Authority to collect PII
- Minimization of PII
- Accounting of disclosures
- System of Records Notices and privacy act statements
- Authorization of systems that are identified as collecting, using, maintaining, or sharing PII
- Dissemination of privacy program information
- Privacy monitoring and auditing
- Privacy reporting
- Privacy awareness and training

See **Appendix III** for an overview of federal privacy criteria evaluated.

The scope of the audit included assessing the implementation of federal privacy requirements for a judgmental sample of three information systems from the total population of 25 information systems in FHFA's FISMA inventory of information systems that required a SORN and a PIA. The scope also included assessing the implementation of federal privacy requirements for a judgmental sample of one information system from the total population of 14 information systems in FHFA-OIG's FISMA inventory of information systems that required a PIA (**Table 2**). The one information system selected for FHFA-OIG also required a SORN.

**Table 2: Description of Systems Selected for Testing**

| Entity | System | Description |
|---|---|---|
| **FHFA** | Employment Matters Tracking | An automated, searchable and secure case tracking mechanism for personnel matters and cases. |
| **FHFA** | FHFA.gov (A Cloud System) | A public facing website designed as a way to communicate the agency's work to FHFA's audiences. Developed with a content management open-source-software to develop, organize and facilitate content creation, hosted in the cloud. |
| **FHFA** | Financial Disclosure Reporting System | The Financial disclosure reporting system is used by FHFA employees to file required confidential financial disclosure reports and for Agency ethics staff to review the reports. |
| **FHFA-OIG** | Office of Investigations Case Management System (OI-CMS) | OI-CMS is the Office of Investigations' central system for holding case file records and managing investigative resources. The system includes documentation from case inception to case closure. |

*Source: Sikich's analysis of the system descriptions in the system inventories and privacy impact analyses.*

The audit also included an evaluation of whether the Agency took corrective action to address open recommendations from the 2023 Privacy audit.[22]

Additionally, Sikich took the following audit into consideration to inform this Privacy 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).

[22] FHFA-OIG Audit Report AUD-2023-006, *Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023).

We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through June 2025.

***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 implemented effective privacy and data protection policies, procedures, and practices, Sikich interviewed key personnel and reviewed legal and regulatory privacy requirements. Also, Sikich reviewed documentation related to the Agency's privacy and data protection program, such as the FHFA's *Privacy Program Plan*, *FHFA-OIG Privacy Program Plan,* and privacy-related policies and procedures, listing of PII holdings, privacy impact assessments, authorization packages for select information systems, privacy continuous monitoring strategy, privacy control assessments, technical controls related to data protection, privacy-related reports, and privacy training materials. In addition, Sikich tested privacy-related processes to determine if the Agency implemented federal privacy requirements (See **Appendix III**).

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 2018 Revision* (Technical Update April 2021).[23]
- The Privacy Act of 1974, 5 U.S.C. Section 552a (January 2009).
- 42 U.S.C. § 2000ee–2, *Privacy and Data Protection Policies and Procedures* (January 2023).
- Section 208 of the e-Government Act of 2002 (December 2002).
- OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020).
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* (December 10, 2020).
- Agency policies and procedures, including but not limited to:
    - FHFA's *Privacy Program Plan* (April 2024).
    - FHFA's *Privacy Continuous Monitoring Strategy*, Revision 2.2 (February 13, 2024).
    - FHFA's *Common Control Plan* (November 21, 2024).
    - *FHFA-OIG Privacy Program Plan* (September 25, 2023).

Sikich evaluated the four systems selected privacy controls to support the assessment of the Agency's implementation of federal privacy requirements. Specifically, Sikich judgmentally

[23] While GAO issued *Government Auditing Standards 2024 Revision* in February 2024, the 2018 revision was still applicable as FHFA-OIG had not implemented the 2024 revision at the time of this audit. Full implementation of the 2024 revision is for audits beginning on or after December 15, 2025.

selected three FHFA information systems based on risk from the total population of 25 information systems in FHFA's FISMA inventory of information systems that required a SORN and a PIA for testing. The systems selected were moderate categorized systems[24] that had PIAs and SORNs and were not tested in prior Privacy Program audits since 2019.

Additionally, Sikich judgmentally selected one FHFA-OIG information system from the total population of 14 information systems in FHFA-OIG's FISMA inventory of information systems that require a PIA. The system selected was a moderate categorized system that had a PIA and SORN and was not tested in prior Privacy Program audits since 2023. Further, the system selected was not in-scope for the 2025 FISMA Audit.

[24] The selected systems were categorized as moderate impact based on NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. Moderate level is the highest categorization FHFA has categorized their information systems.

## APPENDIX III: DETAILED TEST RESULTS

The table below summarizes the federal privacy requirements we reviewed for the Agency's privacy and data protection program and practices, mapped to applicable privacy controls outlined in NIST SP 800-53, Revision 5.[25] We evaluated the following entity and system-level federal privacy requirements to conclude on the Agency's privacy and data protection program and practices. See the below table for our conclusions on tests performed during the audit.

| # | Federal Criteria | NIST SP 800-53 Control(s) | Results |
|---|---|---|---|
| 1 | **OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-A**<br>FHFA establishes and maintains a comprehensive privacy program that (1) ensures compliance with applicable privacy requirements, (2) develops and evaluates privacy policy, and (3) manages privacy risks.<br><br>**OMB Circular A-130, Section 5 Policy, Subsection F Privacy and Information Security – 1-B**<br>Designate an SAOP who has agency-wide responsibility and accountability for (1) developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems; (2) developing and evaluating privacy policy; and (3) managing privacy risks at the agency.<br><br>**OMB Circular A-130, Appendix I, Section 4 Specific Requirements, C-2**<br>Develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the (1) structure of the privacy program, (2) resources dedicated to the privacy program, (3) role of the SAOP and other privacy officials and staff, (4) strategic goals and objectives of the privacy program, (5) program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and (6) any other information determined necessary by the agency's privacy program.<br><br>**OMB Circular A-130, Appendix I-Section 4, Specific Requirement, E-5**<br>Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency. | PM-18 Privacy Program Plan<br><br>PM-19 Privacy Program Leadership Role | **No exceptions noted.** |

[25] Privacy controls are incorporated within NIST SP 800-53, Revision 5, available online here.

| # | Federal Criteria | NIST SP 800-53 Control(s) | Results |
|---|---|---|---|
| 2 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Assure that technologies used to collect, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program. | SC-8 Transmission Confidentiality and Integrity<br><br>SC-28 Protection of Information at Rest | **No exceptions noted.** |
| 3 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form. | None | Recommendations 11, 12, and 13 in 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 loss prevention controls. |
| 4 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Handle personal information contained in Privacy Act systems of records in full compliance with fair information practices as defined in the Privacy Act of 1974 [5 U.S.C. 552a].<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information**<br>Ensure the SAOP reviews and approves the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, in accordance with NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*. | PM-5(1) System Inventory \| Inventory of Personally Identifiable Information<br><br>PM-27 Privacy Reporting | **No exceptions noted.** |
| 5 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Conduct a PIA of proposed rules of the agency on the privacy of information in an identifiable form, including the type of PII collected and the number of people affected.<br><br>**Section 208 of the E-Government Act of 2002**<br>Conduct PIAs of information technology and collections and, in general, make PIAs publicly available.<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-l** | RA-8 Privacy Impact Assessments | **No exceptions noted.** |

| # | Federal Criteria | NIST SP 800-53 Control(s) | Results |
|---|---|---|---|
| | Conduct privacy impact assessments when developing, procuring, or using IT, in accordance with the E-Government Act and make the privacy impact assessments available to the public in accordance with OMB policy. | | |
| 6 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Prepare a report to Congress on an annual basis on activities of the agency that affect privacy, including complaints of privacy violations, implementation of section 11 U.S.C. 552a of title 5, internal controls, and other relevant matters. | PM-27 Privacy Reporting | **No exceptions noted.** |
| 7 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Protect information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. | SI-1 Policy and Procedures<br><br>MP-6 Media Sanitization<br><br>SI-12 Information Management and Retention<br><br>SI-12 (3) Information Management and Retention \| Information Disposal | **Exceptions noted.**<br><br>**See Findings #1 and #2, and Table 1 in the Executive Summary of this report.** |
| 8 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies. | AT-2 Literacy Training and Awareness<br><br>AT-3 Role-based Training<br><br>PL-4 Rules of Behavior | **No exceptions noted.** |
| 9 | **42 U.S.C § 2000ee–2, Privacy and Data Protection Policies and Procedures**<br>Ensure compliance with the agency's established privacy and data protection policies.<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Section I Risk Management Framework**<br>Ensure the SAOP develops and maintains a privacy continuous monitoring strategy and privacy continuous monitoring program to maintain ongoing awareness of privacy risks. This includes (1) conducting privacy control assessments and (2) identifying metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manages privacy risks**.** | CA-2 Control Assessments<br><br>PM-31 Continuous Monitoring Strategy | **No exceptions noted.** |
| 10 | **Privacy Act of 1974, 5 U.S.C. Section 552a**<br>Collect only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. | PT-2 Authority to Process Personally Identifiable Information | **No exceptions noted.** |

| # | Federal Criteria | NIST SP 800-53 Control(s) | Results |
|---|---|---|---|
| | **OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-D**<br>Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions.<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-F**<br>Take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier. | SA-8 (33) Security and Privacy Engineering Principles \| Minimization<br><br>SI-12 (1) Information Management and Retention \| Limit Personally Identifiable Information Elements | |
| 11 | **Privacy Act of 1974, 5 U.S.C. Section 552a**<br>Protect PII from any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, and do not disclose this information except under certain circumstances. | PM-21 Accounting of Disclosures | **No exceptions noted.** |
| 12 | **Section 208 of the E-Government Act of 2002**<br>Post privacy policies on agency Web sites used by the public.<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-J**<br>Maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy. | PM-20 Dissemination of Privacy Program Information | **No exceptions noted.** |
| 13 | **OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F, Privacy and Information Security, 1-G**<br>Privacy Act System of Records Notices are published, revised, and rescinded, as required. | PT-5 (2) Privacy Notice \| Privacy Act Statements<br><br>PT-6 System of Records Notices | **No exceptions noted.** |
| 14 | **OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix I, Section 4 Specific Requirements, E-8**<br>Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization.<br><br>**OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix I, Section 4 Specific Requirements, E-9**<br>Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks. | None | **No exceptions noted.** |

## APPENDIX IV: STATUS OF PRIOR RECOMMENDATIONS

The recommendations from the 2023 Privacy Program audit, FHFA-OIG Audit Report AUD-2023-006*, Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023) were closed during the FY 2024 FISMA audit.[26]

[26] 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).

## APPENDIX V: MANAGEMENTS COMMENTS

**FHFA's Management Comments**

# Federal Housing Finance Agency

**MEMORANDUM**

TO: James Hodge, Deputy Inspector General for Audits

FROM: Brent Burris, Senior Agency Official for Privacy /s/

SUBJECT: Draft Audit Report: *Performance Audit of the Federal Housing Finance Agency's Privacy and Data Protection Program*

DATE: July 16, 2025

---

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) draft report (Report). The objective of the audit was to assess the Federal Housing Finance Agency's (FHFA or Agency) implementation of its privacy program in accordance with applicable laws, regulations, and policies for the period from April 1, 2023, to March 31, 2025.

We are pleased the audit determined that the Agency generally implemented comprehensive privacy policies, procedures, and practices. FHFA management's responses to the three recommendations in the report are outlined below.

**Recommendation 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.*

**Management Response:** FHFA agrees with the recommendation. The Senior Agency Official for Privacy (SAOP) has confirmed that the system owner reviewed and verified that all approvals for current privileged user accounts in the FHFA.gov production environment are documented.

**Recommendation 2:** *Update FHFA's FHFA.gov Customer Controls to document account management requirements for non-privileged users to include account creation and authorization procedures.*

**Management Response:** FHFA agrees with the recommendation. FHFA notes that individually documented access approvals for non-privileged users (i.e., Authenticated Users) was not and will not be required pursuant to the FHFA.gov Customer Controls document. By September 30, 2025, FHFA will revise the Customer Controls document to clarify that the account creation and authorization process for Authenticated Users is implemented via single sign-on authentication.

**Recommendation 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.*

**Management Response:** FHFA agrees with the recommendation. The SAOP has confirmed that the system owner implemented additional logging capabilities to capture access and deactivation events for all user accounts.

If you have any questions, please contact me at (202) 649-3037 or by email at Brent.Burris@fhfa.gov.

cc: Clinton Jones
Tallman Johnson
Luis Campudoni
Jeffery Harris
John Major

## FHFA-OIG's Management Comments

**OFFICE OF INSPECTOR GENERAL**
**Federal Housing Finance Agency**

400 7th Street SW, Washington, DC 20219

July 3, 2025

**TO:** Sikich

**FROM:** Mary B. Schaefer, Acting Chief Counsel /s/

**SUBJECT:** Audit Report: Federal Housing Finance Agency and the Federal Housing Finance Agency Office of Inspector General's Privacy and Data Protection Policies and Procedures for 2025.

We are in receipt of Sikich's audit report for the Federal Housing Finance Agency and the Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) Privacy and Data Protection Policies and Procedures for 2025. FHFA-OIG trusts that the results of this independent audit will provide assurance to our stakeholders that FHFA-OIG's Privacy Program and practices are operating in accordance with federal law and regulation.

We appreciate Sikich's work on the report and professionalism in conducting this year's audit. If you have any questions, please feel free to contact me at mary.schaefer@fhfaoig.gov.

## APPENDIX VI: ABBREVIATIONS

| | |
|---|---|
| FHFA | Federal Housing Finance Agency |
| FHFA-OIG | FHFA Office of Inspector General |
| FISMA | Federal Information Security Modernization Act |
| NIST | National Institute of Standards and Technology |
| OCAC | Office of Congressional Affairs and Communication |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| SAOP | Senior Agency Official for Privacy |
| Sikich | Sikich CPA LLC |
| SORN | System of Records Notice |
| SP | Special Publication |
| U.S.C. | United States Code |

# 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