Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023

Audit Report • AUD-2023-006 • August 23, 2023

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

August 23, 2023

TO: Sandra L. Thompson, Director

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

SUBJECT: Audit Report, *Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (AUD-2023-006)

We are pleased to transmit the subject report.

Title 42 United States Code § 2000ee-2, Privacy and Data Protection Policies and Procedures (Privacy and Data Protection Code), 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, the Privacy and Data Protection Code requires the Office of Inspector General (OIG) to periodically conduct a review of the Federal Housing Finance Agency's (FHFA) implementation of this section and report the results of our review to the Congress.

We contracted with CliftonLarsonAllen LLP (CLA), a certified independent public accounting firm, to conduct the fiscal year 2023 performance audit of the Federal Housing Finance Agency's and the FHFA Office of Inspector General's (collectively, the Agency) privacy and data protection programs and practices. CLA conducted its audit in accordance with generally accepted government auditing standards.

Based on its audit, CLA concluded that the Agency had 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, consistent with legal and regulatory guidance. However, the Agency did not fully achieve implementation of certain privacy requirements.

Specifically, CLA reported four findings:

(1) FHFA-OIG Needs to Strengthen Its Privacy Training Program;

(2) FHFA Needs to Improve Its Privacy Impact Assessment Process;

(3) FHFA Needs to Determine Required Privacy Impact Assessments for Agency Proposed Rules; and

(4) FHFA Needs to Update Its Privacy Continuous Monitoring Strategy.

To address these findings, CLA made five new recommendations and reaffirmed one recommendation from a prior OIG audit.

In connection with the contract, we reviewed CLA'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 and related information security policies, procedures, standards, and guidelines. CLA is responsible for the attached audit report dated August 3, 2023, and the conclusions expressed therein. Our review found no instances where CLA did not comply, in all material respects, with generally accepted government auditing standards.

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

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Privacy Program,
Fiscal Year 2023

Audit of the Federal Housing Finance Agency's Privacy Program

Fiscal Year 2023

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

August 3, 2023

The Honorable Brian M. Tomney
Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Inspector General Tomney:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG's) implementation of privacy and data protection policies, procedures, and practices, as directed in 42 United States Code (U.S.C.) § 2000ee-2. Our report presents FHFA's and FHFA-OIG's combined results (collectively referred to as the Agency). We performed this audit under contract with the FHFA-OIG.

We have reviewed the Agency's responses to a draft of this report and included our evaluation of managements' 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.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
Federal Housing Finance Agency

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG's), collectively referred to as the Agency for reporting combined results, implementation of privacy and data protection policies, procedures, and practices, as directed in 42 United States Code (U.S.C.) § 2000ee-2.

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection programs and practices in accordance with law, regulation, and policy. Specifically, the audit was designed to determine whether the Agency 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, consistent with legal and regulatory guidance.

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.

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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. NIST's 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, and Office of Management and Budget (OMB) memoranda. In addition, the audit included an assessment of the implementation of federal privacy requirements for a sample of three FHFA systems from the total population of 22 FHFA systems that collected personally identifiable information (PII) and one FHFA-OIG system from the total population of 14 FHFA-OIG systems that require a privacy impact assessment.

The audit also included evaluating whether FHFA took corrective actions to address privacy-related findings and recommendations in FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021).[1]

The scope of this performance audit covered the Agency's privacy and data protection programs and practices from April 1, 2021, through March 31, 2023. We conducted audit fieldwork remotely from October 2022 through July 2023.

We concluded that collectively the Agency had 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

[1] See report online here.

agency employees and the public, consistent with legal and regulatory guidance. However, while the Agency generally implemented comprehensive privacy and data protection policies, procedures, and practices, the Agency's implementation of certain privacy requirements was not fully achieved. We noted weaknesses in privacy role-based training, privacy impact assessments, proposed rules, and privacy continuous monitoring strategy. As such, we made five new recommendations and reaffirmed one prior privacy audit recommendation to assist the Agency in strengthening its privacy and data protection programs and practices.

Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

Arlington, Virginia
August 3, 2023

Table of Contents

EXECUTIVE SUMMARY 1

Summary of Results 2

AUDIT FINDINGS 4

1. FHFA-OIG Needs to Strengthen Its Privacy Training Program 4

2. FHFA Needs to Improve Its Privacy Impact Assessment Process 5

3. FHFA Needs to Determine Required Privacy Impact Assessments for Agency Proposed Rules 7

4. FHFA Needs to Update Its Privacy Continuous Monitoring Strategy 8

EVALUATION OF MANAGEMENTS' COMMENTS 10

APPENDIX I: BACKGROUND 12

APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY 14

APPENDIX III: DETAILED TEST RESULTS 18

APPENDIX IV: STATUS OF PRIOR RECOMMENDATIONS 24

APPENDIX V: MANAGEMENTS' COMMENTS 26

EXECUTIVE SUMMARY

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged CliftonLarsonAllen LLP (CLA) 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, procedures, and practices, as directed in 42 United States Code (U.S.C.) § 2000ee-2. The audit meets the requirement in 42 U.S.C. § 2000ee-2 that Inspectors General periodically review their respective agencies' privacy and data protection programs and practices.

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection programs and practices 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, 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, consistent with legal and regulatory guidance. In addition, the audit included evaluating whether FHFA took corrective actions to address privacy-related findings and recommendations in FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021).

The scope of this performance audit covered the Agency's privacy and data protection programs and practices from April 1, 2021, through March 31, 2023. We conducted audit fieldwork remotely from October 2022 through July 2023.

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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.[2] 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, Office of Management and Budget (OMB) memoranda, and NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

The audit also included an assessment of the implementation of federal privacy requirements for a sample of three[3] FHFA systems from the total population of 22 FHFA systems that collected personally identifiable information (PII) and one FHFA-OIG[4] system from the total population of 14 FHFA-OIG systems that require a privacy impact assessment (PIA).

We conducted this performance audit in accordance with the 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.

[2] See Appendix III for mapping of controls.

[3] We sampled the following FHFA Privacy Systems: Emergency Notification System, National Mortgage Database and a cloud system. See Appendix II, Table 2 for a description of the systems.

[4] We sampled the following FHFA-OIG System: OIGNet General Support System. See Appendix II, Table 2 for a description of the system.

Summary of Results

Progress Since 2021

At the beginning of fiscal year 2023, there were five open privacy recommendations from the 2021 Privacy audit.[5] During the course of the audit, we found that FHFA took corrective actions to address four recommendations, and we consider those recommendations closed. Corrective actions are in progress on the one open recommendation. Refer to Appendix IV for a detailed description of the status of each recommendation.

Current Status

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, consistent with legal and regulatory guidance. Specifically, we noted that the Agency had implemented the following privacy and data protection requirements:

- Designating a Senior Agency Official for Privacy (SAOP) (as referred to as Chief Privacy Officer) with responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program.
- Documenting and maintaining current System of Records Notices.[6]
- Reporting annually on the activities of the agency that affect privacy.
- Reviewing and approving the categorization of information systems that collect, house, or utilize PII in accordance with Federal Information Processing Standards.
- 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 was not fully achieved. We noted weaknesses in privacy role-based training, privacy impact assessments, proposed rules, and privacy continuous monitoring strategy (**Table 1**). As such, we made five new recommendations and reaffirmed one prior privacy audit recommendation to assist the Agency in strengthening its privacy and data protection programs and practices.

In a response to a draft of this report, FHFA and FHFA-OIG provided separate management responses related to their specific findings and recommendations. FHFA and FHFA-OIG management agreed with all five new recommendations made in this report; and outlined their plans and the corrective actions taken to address each new recommendation and the reaffirmed prior recommendation from 2021.[7]

---

[5] FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021). See report online here.

[6] A System of Records Notices (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 (SOR).

[7] Recommendation 3, FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021). See report online here.

Table 1: Summary of Findings and Recommendations

Privacy Program Weaknesses	Recommendations
1. FHFA-OIG Needs to Strengthen Its Privacy Training Program.	**Recommendation 1:** We recommend that FHFA-OIG's Chief Counsel update the *FHFA-OIG Privacy Program Plan* to include procedures to verify personnel's completion of annual role-based privacy training. Procedures should include periodic progress checks and follow-up with personnel to ensure timely training completion.
2. FHFA Needs to Improve Its Privacy Impact Assessment Process.	**Recommendation 2:** We recommend that FHFA's SAOP revise the *FHFA Privacy Program Plan* to document the frequency of review for existing PIAs in accordance with OMB Circular No. A-130. **Recommendation 3:** We recommend that FHFA's SAOP, in coordination with the System Owner and the Chief Information Security Officer (CISO), ensure that all required approval signatures are captured within the PIA and maintain a record of review for each PIA, as required by the *FHFA Privacy Impact Assessment Guide.* **Recommendation 4:** We recommend that FHFA's SAOP update the PIAs for the Emergency Notification System, the National Mortgage Database (NMDB), and the cloud system to ensure PIAs accurately describe all security and privacy controls of the system and are approved by the required officials.
3. FHFA Needs to Determine Required Privacy Impact Assessments for Agency Proposed Rules.	**Recommendation 5:** We recommend that FHFA's SAOP, in coordination with the originating office and the Office of General Counsel, obtain and review proposed rules, and determine if a PIA is required, in accordance with FHFA Policy No. 801, *Official Documents Policy*.
4. FHFA Needs to Update Its Privacy Continuous Monitoring Strategy.	We reaffirm a recommendation from the 2021 audit report:[8] **AUD-2021-011, Recommendation 3:** FHFA's SAOP update the *Privacy Continuous Monitoring Strategy* to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular No. A-130.

The following section provides additional information on the audit findings. Appendix I provides background information on the Agency's privacy and data protection programs, practices, and appliable federal privacy policies. Appendix II describes the audit objective, scope, and methodology. Appendix III provides detailed test results and Appendix IV provides the status of prior recommendations. Appendix V includes the Agency's comments.

[8] See footnote 7.

AUDIT FINDINGS

1. FHFA-OIG Needs to Strengthen Its Privacy Training Program

According to the FHFA-OIG's training records as of February 7, 2023, only 39 percent (28 of 72) of personnel, whose responsibilities include access to PII, completed the required annual role-based privacy training by the due date of December 30, 2022. The oversight was identified on January 20, 2023, upon CLA's request for role-based privacy training records. Upon notification, FHFA-OIG took action to train all required personnel. However, FHFA-OIG lacks procedures to verify the completion of the role-based privacy training.

An FHFA-OIG official stated that the annual role-based privacy training was inadvertently not assigned to the learning plans in the electronic training system, Learning Management System (e-LMS) for all required personnel. The e-LMS system requires manual input to update users' learning plans with required training. In addition, the FHFA-OIG's Mandatory Training Course e-mail, sent on November 30, 2022, informed recipients that the annual training requirement course: *2022 FHFA-OIG Role-Based Privacy Training* was assigned to personnel learning plans in e-LMS with a due date of December 30, 2022. However, the e-mail notification was not sent to all required personnel.

NIST SP 800-53, Revision 5, security control Awareness and Training (AT)-3, Role-Based Training, requires that agencies provide role-based security and privacy training to personnel with assigned roles and responsibilities (1) before authorizing access to the system, information, or performing assigned duties; (2) when required by system changes; and (3) on an organization-defined frequency thereafter.

Consistent with the NIST requirements, the *FHFA-OIG Privacy Program Plan*, version 4 (July 2022), requires FHFA-OIG to provide targeted, role-based training to those employees, supervisors, and contractor personnel with specialized roles who use, view, or have access to PII in the routine performance of their jobs; administer role-based privacy training annually to appropriate FHFA-OIG staff and contractors; and document privacy training completion dates in its e-LMS to ensure all staff and contractor participation as required.

According to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*[9] (September 2014) (Control Activities, Principles 12.02, 12.03, 12.04) management should implement control activities through policies. Management for the unit may further define policies through day-to-day procedures. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified. Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

Without annual privacy role-based training, personnel may be unaware of new requirements or changes to existing privacy requirements, policies, and procedures, increasing the risk of mishandling PII or improperly performing their privacy-related duties.

[9] See GAO *Standards for Internal Control in the Federal Government* (the "Green Book") online here.

We recommend that FHFA-OIG's Chief Counsel do the following:

> ***Recommendation 1:*** *Update the FHFA-OIG Privacy Program Plan to include procedures to verify personnel's completion of annual role-based privacy training. Procedures should include periodic progress checks and follow-up with personnel to ensure timely training completion.*

2. FHFA Needs to Improve Its Privacy Impact Assessment Process

FHFA did not conduct periodic reviews of its PIAs, as required by OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016).[10] Specifically, we found the following related to FHFA's PIAs:

1. Two out of the three systems selected for testing, that collect PII, had PIAs that were not reviewed for updates since the PIAs were initially developed and approved, and contained outdated information. For example:

    - The Emergency Notification System[11] PIA (June 14, 2016) stated that the System of Records Notices[12] will need to be updated to reflect new data elements collected, a new vendor location, and storage location. However, the PIA has not yet been updated to reflect that FHFA had already published a revised System of Records Notices on April 15, 2016, to address the required changes.
    - The NMDB[13] PIA (November 6, 2013) stated that the System of Records Notices is in the process of being revised to reflect additional data fields that are being collected. However, the PIA has not yet been updated to reflect that FHFA had already published a revised System of Records Notices on August 28, 2015, to address the required changes.

2. The cloud system[14] PIA (April 12, 2021) was not reviewed and signed by all officials. For example, the Senior Agency Information Security Officer (also referred to as the CISO) did not review and sign the PIA, to ensure that information technology (IT) security issues and safeguards are properly addressed, as required by the *FHFA Privacy Program Plan* (July 2022).

An FHFA Privacy Office official stated that there were no changes to all three systems that required the PIA to be updated; however, this determination was not documented and therefore,

---

[10] See OMB Circular No. A-130 online here.

[11] According to the FHFA Customer Controls for the Emergency Notification System (July 7, 2022), Emergency Notification System is a cloud-hosted service that utilizes contact information for all agency users to distribute notifications to agency users in real-time via text, voice or email regarding incidents that may impact mission critical offices and employees.

[12] According to the *FHFA Privacy Program Plan*, FHFA must create a System of Records Notices when (i) an information system contains records that include PII, (ii) the records are under the control of FHFA, and (iii) the records are retrieved using an individual's name or other unique identifier.

[13] According to the *FHFA System Security Plan for the NMDB* (April 25, 2019), NMDB is designed to provide a rich source of information about the U.S. mortgage market. The NMDB enables FHFA to conduct a monthly mortgage market survey to collect data on the characteristics of individual mortgages and collect information on the creditworthiness of borrowers.

[14] According to the FHFA Customer Controls for the cloud system (August 31, 2022), the cloud system is a Federal Risk and Authorization Management Program (FedRAMP) authorized software-as-a-service (SaaS) solution administered from a cloud-based environment and provides intuitive budgeting, staffing, forecasting, reporting, and dashboards.

could not be substantiated. The same Privacy Office official also stated that during FHFA's *Privacy Program Plan* review in July 2022, FHFA omitted the frequency of review for existing PIAs because there was not a corresponding NIST SP 800-53, Revision 5, control for them to document their review schedule. The same FHFA Privacy Office official stated that FHFA will be operating under a three-year review cycle for PIAs; however, this is not reflected within FHFA's *Privacy Program Plan*. The same FHFA Privacy Office official stated that the outdated PIAs were reviewed to determine the review schedule priority. The FHFA Privacy Office's review schedule is prioritized in their *Workplan* in the order of risk.

According to FHFA officials, the CISO did not review and sign the cloud system PIA because the CISO had already reviewed and signed the cloud system's Authority to Operate[15] memorandum on March 30, 2021, which assessed the security and privacy controls for the system. In addition, FHFA officials stated that the Privacy Office had updated its internal processes to ensure that all future PIAs have all signatures listed on the form or not applicable designations as appropriate.

OMB Circular No. A-130 states that the SAOP shall assess the privacy controls periodically at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a PIA is a living document that agencies are required to update whenever changes to the information technology, changes to the organization's practices, or other factors alter the privacy risks associated with the use of such information technology.

FHFA's *Privacy Program Plan* (July 2022) provides an overview of the requirements for the privacy program and a description of the privacy program management controls in place for meeting those requirements. The *FHFA Privacy Program Plan* states that a PIA is an assessment of how PII is handled. PIAs are used to identify and address privacy issues in planning, developing, and implementing IT systems that collect and maintain PII. Further, it requires Information and System Owners to coordinate with the system developer, if applicable, IT Security Team, and Privacy Office, to complete a PIA whenever FHFA (1) initiates a new electronic collection of PII; (2) develops or procures an IT system that collects, maintains, or disseminates PII from or about members of the public; or (3) when significant changes are made in how PII is managed in an electronic system. If a PIA is required, the Information or System Owner conducts and completes a PIA and submits it to the Privacy Office for review. The SAOP, or their designee, works with the Information or System Owner and CISO to resolve any privacy or IT security risks described in the PIA. Once finalized and signed by all required parties, the PIA is posted to FHFA's public website and copies are provided to the Information or System Owner, SAOP, and CISO.

As referenced in the *FHFA Privacy Program Plan*, the *FHFA Privacy Impact Assessment Guide* states the CISO is responsible for reviewing the PIA to ensure that IT security issues and safeguards are properly addressed, and the SAOP is responsible for reviewing and approving the PIA to ensure that privacy issues and safeguards are properly addressed. Further, the system owner, CISO and SAOP are responsible for obtaining the appropriate approvals and retain a copy of the final documents.

[15] According to NIST SP 800-53, Revision 5, an Authority to Operate is an official management authorization decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

Failure to review and update PIAs on a timely basis increases the risk that privacy risks may not be completely accounted for, and properly mitigated, which may increase the risk of loss or mishandling of PII or other sensitive information. In addition, the absence of complete signatures may indicate officials' lack of involvement with the review of the PIA to ensure that IT security and privacy issues and safeguards are properly addressed to mitigate privacy risks.

We recommend that FHFA's SAOP do the following:

> ***Recommendation 2:*** *Revise the FHFA Privacy Program Plan to document the frequency of review for existing PIAs in accordance with OMB Circular No. A-130.*
>
> ***Recommendation 3:*** *In coordination with the System Owner and CISO, ensure that all required approval signatures are captured within the PIA and maintain a record of review for each PIA, as required by the FHFA Privacy Impact Assessment Guide.*
>
> ***Recommendation 4:*** *Update the PIAs for the Emergency Notification System, the NMDB, and the cloud system to ensure PIAs accurately describe all security and privacy controls of the system and are approved by the required officials*.

3. FHFA Needs to Determine Required Privacy Impact Assessments for Its Proposed Rules

FHFA's Chief Privacy Officer did not review all proposed rules[16] of the FHFA to determine if a PIA is required, as specified by 42 U.S.C. § 2000ee-2. *Privacy and Data Protection Policies and Procedures*. Specifically, the FHFA Chief Privacy Officer did not review four of the seven proposed rules issued during the audit period to determine whether a PIA was required. Upon notification, the FHFA Chief Privacy Officer took action, and stated that FHFA reviewed the remaining four proposed rules and determined that one of the four remaining proposed rules may require a PIA before it is published as a final rule.[17]

A FHFA Privacy Office official confirmed that the Office of Capital Policy and the Office of General Counsel did not include the FHFA Chief Privacy Officer in the analysis, development, and review of proposed rules due to oversight.

42 U.S.C. § 2000ee-2. *Privacy and Data Protection Policies and Procedures*[18] states the Chief Privacy Officer assumes the primary responsibility for privacy and data protection policy, including conducting a PIA 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.

FHFA Policy No. 801, *Official Documents Policy*, states the *Official Documents Policy* (June 8, 2018) provides Agency principles for developing Official Documents and Agency procedures for clearing Official Documents. Official Documents includes documents concerning the entities that

---

[16] The Office of the Federal Register defines "proposed rule," or "Notice of Proposed Rulemaking", as an official document that announces and explains the agency's plan to address a problem or accomplish a goal.

[17] The proposed rule is published to the Federal Registrar for the public to participate in the rulemaking process by providing comments. The comments are used by FHFA in their process to update, as necessary, and finalize the rule. During this time, when FHFA is reviewing comments and updating the rule for finalization, a privacy review would occur and a PIA would be developed, if necessary.

[18] See 42 USC 2000ee-2: Privacy and data protection policies and procedures online here.

FHFA oversees: such documents establish regulatory or conservatorship requirements and guidance or provide other applicable information. Further, the *Official Documents Policy* requires the originating Office[19] should be inclusive in seeking stakeholder involvement from other Divisions and Offices in analyzing, developing, and reviewing Official Documents. Further, the originating Office is responsible for routing clearance packages to stakeholder Divisions and Offices for clearance.

Additionally, as stated in *Official Documents Policy*, Appendix D: *Requirements for Developing Regulations* (including proposed, final, and interim final rules, and Advanced Notices of Proposed Rulemaking), when FHFA is developing the regulation, each project is to have two leads: one from Office of General Counsel and one from the relevant line Office. Furthermore, stakeholders should be those Division or Office leads whose input the Director would reasonably expect to have the benefit of before being asked to approve the regulation package, including for all regulations, the Chief Privacy Officer is a stakeholder who may determine whether a PIA is required.

Without the FHFA Chief Privacy Officer's review of proposed rules for PIA determination, FHFA may collect new information or change the way that information is used that would increase the privacy risks to the FHFA.

We recommend that FHFA's SAOP do the following:

> ***Recommendation 5:*** *In coordination with the originating office and the Office of General Counsel, obtain and review proposed rules, and determine if a PIA is required, in accordance with FHFA Policy No. 801*, *Official Documents Policy.*

4. FHFA Needs to Update Its Privacy Continuous Monitoring Strategy

In the 2021 audit of the FHFA's privacy and data protection program,[20] it was noted that FHFA's *Privacy Continuous Monitoring Strategy* (September 2020) did not completely describe FHFA's privacy control monitoring process. Specifically, the strategy stated that privacy control assessments were included in the information security continuous monitoring (ISCM)[21] process. However, in practice, the scheduling, testing, and reporting of privacy controls were performed separately, outside of the ISCM process, by the SAOP.

During our 2023 Privacy audit testing, we noted that FHFA's Privacy Office strengthened their privacy monitoring processes by introducing a *Workplan*[22] process, in addition to the control

---

[19] Per the FHFA Policy No. 801, *Official Documents Policy*, the Originating Office is the FHFA Division or Office responsible for initiating the Official Document and the clearance package in collaboration with stakeholders, ensuring its completion and, typically, implementing its requirements. In most cases, there will be only one originating Office; however, there are circumstances in which there are co-originating Offices. For example, the Office of the General Counsel is a co-originating Office on regulations with the Division or Office that is the policy or supervision lead.

[20] See footnote 7.

[21] FHFA's *Privacy Continuous Monitoring Strategy* (September 2020), stated that: FHFA performs ongoing control assessments in accordance with the ISCM Ongoing Assessment Schedule maintained by the ISCM Team. Privacy controls are included in the ISCM Ongoing Assessment Schedule. The schedule will be reviewed and updated, as appropriate and at minimum annually, to ensure the selection of controls and frequency of assessments continue to meet established requirements to maintain operations within organizational risk tolerances.

[22] FHFA's Privacy Office *Workplan* (initially created in April 2021) is used to continuously monitor the privacy program, including system specific review of privacy impact assessments, which includes a reference to any relevant System of Records Notices.

assessment process performed by Office of Technology and Information Management. The *Workplan* process details the Privacy Office's privacy monitoring activities and scheduling the remediation of self-identified operational deficiencies to implement tighter controls. However, the processes around the *Workplan* were not detailed in FHFA's *Privacy Continuous Monitoring Strategy* (April 29, 2022).

Our testing reaffirmed the prior year finding, as part of FHFA's current privacy control monitoring process was performed separately, outside of the Office of Technology and Information Management ISCM control assessment process, by the Privacy Office and tracked in its *Workplan*. As such, FHFA did not implement the recommendation to update the *Privacy Continuous Monitoring Strategy* to completely describe its privacy control assessment process.

An FHFA Privacy Office official acknowledged that the *Privacy Continuous Monitoring Strategy* does not include the privacy control assessment processes, related to the Privacy Office's privacy control monitoring activities, that is documented within their *Workplan*. The same official stated that the Privacy Office continues to be in the process of updating policies and procedures to include new Privacy Office initiatives, like the *Workplan*. In a written statement, it is noted that the Privacy Office started developing the *Workplan* in April 2021, when the new SAOP was hired. Over time, the scope of the *Workplan* evolved to mitigate self-identified operational deficiencies to implement tighter controls. The evolution of the *Workplan* took time, as the Privacy Office had to incorporate operational improvements into privacy system reviews and provide legal counsel on agency Privacy Act matters. The Privacy Office expects to increase the process improvement rate of change with the addition of a new attorney for Privacy and Freedom of Information Act.

OMB Circular No. A-130 includes requirements and responsibilities for protecting federal information resources and managing PII. OMB A-130, Appendix II, Section I, *Risk Management Framework*, requires that the SAOP develops and maintains a privacy continuous monitoring strategy and privacy continuous monitoring program to maintain ongoing awareness of privacy risks.

NIST SP 800-53, Revision 5, provides a catalog of security and privacy controls. NIST control Program Management (PM)-18, *Privacy Program Plan* requires organizations to develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program that includes a description of the structure of the privacy program and the resources dedicated to the privacy program; and provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements.

Without completely describing the privacy control assessment process in the FHFA's *Privacy Continuous Monitoring Strategy*, there may be an increased risk that privacy control assessment and monitoring of controls will not be performed timely or adequately to address privacy risks.

We reaffirm a recommendation from the 2021 audit report[23] that FHFA's SAOP do the following:

> ***AUD-2021-011, Recommendation 3:*** *Update the Privacy Continuous Monitoring Strategy to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular No. A-130.*

[23] See footnote 7.

EVALUATION OF MANAGEMENTS' COMMENTS

In response to a draft of this report, FHFA and FHFA-OIG provided separate management responses related to their specific program's findings and recommendations. FHFA and FHFA-OIG management agreed with all five new recommendations in this report; and outlined their plans and the corrective actions taken to address each new recommendation and the reaffirmed prior year recommendation from 2021.[24] Appendix V includes the Agency's comments.

FHFA-OIG Response:

For recommendation 1, FHFA-OIG management agreed with the recommendation. FHFA-OIG management stated that it will finalize the update of its *Privacy Program Plan* to include specific steps to ensure and verify completion of annual role-based privacy training by all personnel required to complete the training. FHFA-OIG expects these actions to be completed by September 30, 2023. FHFA-OIG's planned corrective actions meet the intent of our recommendation.

FHFA Response:

For recommendation 2, FHFA management agreed with the recommendation. FHFA management stated that it revised the *FHFA Privacy Program Plan* in July 2023 to document FHFA's review frequency for existing PIAs. FHFA's corrective actions meet the intent of our recommendation. Because the corrective actions occurred after the scope of our audit, the remediation of this recommendation will be evaluated in the next privacy audit.

For recommendation 3, FHFA management agreed with the recommendation. FHFA management stated that it implemented an electronic clearance process to ensure that all required approvals are captured on the PIA, serving as the record of review for each PIA. The PIA electronic clearance process was documented in the *FHFA Privacy Impact Assessment Guide* in April 2023. FHFA's corrective actions meet the intent of our recommendation. Because the corrective action occurred after the scope of our audit and the approving of PIAs is an ongoing control, the remediation of this recommendation will be evaluated in the next privacy audit.

For recommendation 4, FHFA management agreed with the recommendation. FHFA management stated that it will update the Emergency Notification System, NMDB, and the cloud system PIAs to ensure that the PIAs accurately describe all security and privacy controls of the system and are approved by the required officials by November 30, 2023. FHFA's planned corrective actions meet the intent of our recommendation.

For recommendation 5, FHFA management agreed with the recommendation. FHFA management stated that the Privacy Office emphasized its role in the rulemaking during the FHFA 2023 annual privacy training that was required to be completed by FHFA staff by June 30, 2023. In addition, the Privacy Office is working with the Office of General Counsel to ensure that the Privacy Office is included in the electronic clearance process for all rulemakings before they are published in the Federal Register. FHFA will ensure that determinations of the need for a PIA in rulemakings are documented as required by the *Official Documents Policy* by November 30, 2023. FHFA's planned corrective actions meet the intent of our recommendation.

[24] See footnote 7.

For the reaffirmed 2021 recommendation (AUD-2021-011, Recommendation 3*),* FHFA management stated that the Privacy Office updated the *Privacy Continuous Monitoring Strategy* to reference the privacy review tracking mechanism in June 2023. FHFA's corrective actions meet the intent of our recommendation. Because the corrective action occurred after the scope of our audit, the remediation of this recommendation will be evaluated in the next privacy audit.

BACKGROUND

Federal Privacy Requirements

The following provides a high-level summary of the key 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.

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 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*

NIST SP 800-37, Revision 2, provides guidelines for applying the Risk Management Framework to information systems and organizations. The Risk Management Framework provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

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.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*

NIST SP 800-122 explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using the Fair Information Practices, which are the principles underlying most privacy laws and privacy best practices. The NIST publication also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.

OBJECTIVE, SCOPE, AND METHODOLOGY

FHFA-OIG engaged CLA 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 programs and practices.

Objective

The objective of this performance audit was to assess the Agency's implementation of its privacy and data protection programs and practices 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, 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, consistent with legal and regulatory guidance.

Scope

The scope of this performance audit covered the Agency's privacy and data protection programs and practices from April 1, 2021, through March 31, 2023.[25] 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 programs 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; OMB and NIST guidance.

The audit included tests of the Agency's compliance with federal privacy laws, regulations, standards, and the Agency 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.[26] 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:

- 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-enhanced system design and development
- Privacy reporting
- Privacy awareness and training

[25] The scope of this audit covered the period since the FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021).

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

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

The scope period also included assessing the implementation of federal privacy requirements for a sample of three information systems from the total population of 22 FHFA systems that collected PII and for a sample of one information systems from the total population of 14 FHFA-OIG systems that require a PIA (**Table 2**).

Table 2: Description of Systems Selected for Testing

Entity	System	Description
FHFA	Emergency Notification System	A cloud-hosted service that utilizes contact information for all agency users to distribute notifications to agency users in real-time via text, voice, or email regarding incidents that may impact mission critical offices and employees.
FHFA	National Mortgage Database	NMDB is designed to provide a rich source of information about the U.S. mortgage market. The NMDB enables FHFA to conduct a monthly mortgage market survey to collect data on the characteristics of individual mortgages and collect information on the creditworthiness of borrowers.
FHFA	A Cloud System	A cloud-based system that provides intuitive budgeting, staffing, forecasting, reporting, and dashboards.
FHFA-OIG	OIGNet General Support System	The FHFA OIGNet General Support System is a general purpose, multi-user system used throughout FHFA-OIG. It is composed of users primarily with desktops and laptops and other ancillary equipment connected via FHFA-OIG network to central servers that support FHFA-OIG. The core network infrastructure consists of network switches, firewalls, and routers that provide boundary protection and network segmentation.

The audit also included an evaluation of whether FHFA took corrective action to address open recommendations from the 2021 Privacy audit.[27]

We conducted audit fieldwork remotely from October 2022 through July 2023.

To accomplish our objective, we determined that three components of GAO's *Standards for Internal Control in the Federal Government* were significant to our objective: management should implement control activities by (1) documenting in policies the internal control responsibilities of the organization, (2) documenting in policies for each unit its responsibility for an operational process's objective and related risks and control activity design, implementation, and operating effectiveness, and (3) those in key roles for the unit may further define polices through day-to-day procedures.[28]

We considered internal controls that were significant and relevant to our audit objective and therefore, we may not have identified all the internal control deficiencies with respect to the Agency's privacy and data protection programs that existed at the time of this audit. Our work did not include an assessment of the sufficiency of internal control over the Agency's privacy and

[27] See footnote 5.

[28] Principle 12 – Implementing Control Activities, Documentation of Responsibilities through Policies 12.02, 12.03, 12.04 in GAO's *Standards for Internal Control in the Federal Government* (September 2014).

data protection programs and practices, or other matters not specifically outlined in this report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information included in this report was obtained from the Agency on or before August 3, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to August 3, 2023.

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, CLA interviewed key personnel and reviewed legal and regulatory privacy requirements. Also, CLA reviewed documentation related to the Agency's privacy and data protection program, such as the *FHFA 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, CLA tested privacy-related processes to determine if the Agency implemented federal privacy requirements (See Appendix III). In addition, CLA reviewed the status of the open privacy-related recommendations, including supporting documentation to ascertain whether the actions taken addressed the weakness. See Appendix IV for the status of prior recommendations.

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

- *Government Auditing Standards* (April 2021).
- GAO's *Standards for Internal Control in the Federal Government* (September 2014).
- 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* (February 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 800-37, Revision 2, *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,* for specification of privacy controls (December 10, 2020).
- NIST SP 800-53A*,* Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of privacy control effectiveness (January 2022).
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*.
- Agency policies and procedures, including but not limited to:
    - *Privacy Continuous Monitoring Strategy* (April 29, 2022).

- *FHFA Privacy Program Plan* (July 2022).
- *FHFA Privacy Impact Assessment Guide* (April 2022).
- *FHFA-OIG Privacy Program Plan* (July 2022).
- FHFA Policy No. 801, *Official Documents Policy* (June 8, 2018).

CLA selected three FHFA systems from the total population of 22 FHFA systems that collected PII. The three systems were selected based on risk. Specifically, three moderate categorized systems[29] were selected, that had not been tested in prior years. Additionally, CLA selected the OIGNet General Support System from the total population of 14 FHFA-OIG systems that require a PIA for testing. The OIGNet General Support System was selected based on risk since it is a moderate categorized system that supports FHFA-OIG applications that reside on the network. CLA tested four systems' selected privacy controls to support the assessment of the Agency's implementation of federal privacy requirements.

In testing for the adequacy and effectiveness of the privacy and data protection program controls and practices, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered the relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population.

[29] Security categorizations are determined by federal agencies using Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, located online here. Federal Information Processing Standards 199 provides a standard for categorizing federal information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

DETAILED TEST RESULTS

The following table (**Table 3)** notes the federal privacy requirements we reviewed for the Agency's privacy and data protection programs and practices, mapped to applicable privacy controls outlined in NIST SP 800-53, Revision 5.[30] We tested the following entity and system-level federal privacy requirements to conclude on the Agency's privacy and data protection programs and practices. See the below table for our conclusions on tests performed during the audit.

Table 3: Detailed Test Results

#	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** 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.	PM-18 Privacy Program Plan PM-19 Privacy Program Leadership Role	**No exceptions noted.**
	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.		**No exceptions noted.**
	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.		**No exceptions noted.**

[30] See footnote 26.

Audit of FHFA's 2023 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control(s)	Results
	Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency.		**No exceptions noted.**
2	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** 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.	None	**No exceptions noted.**
3	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** 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	**No exceptions noted.**
4	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** 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].	PM-5(1) System Inventory | Inventory of Personally Identifiable Information PM-27 Privacy Reporting	**No exceptions noted.**
	OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information 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	**No exceptions noted.**

Audit of FHFA's 2023 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control(s)	Results
5	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** 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.	RA-8 Privacy Impact Assessments	**Exceptions noted.** **See Finding #3 above.**
	Section 208 of the E-Government Act of 2002 Conduct PIAs of information technology and collections and, in general, make PIAs publicly available.	RA-8 Privacy Impact Assessments	**Exceptions noted.** **See Findings #2 and #4 above.** **See Appendix IV – prior year finding - AUD 2021-011, Recommendation #3**
	OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-l 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.	RA-8 Privacy Impact Assessments	**No exceptions noted.**
6	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** 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** Protect information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.	PM-24 Data Integrity Board SI-1 Policy and Procedures MP-6 Media Sanitization	**No exceptions noted.**

Audit of FHFA's 2023 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control(s)	Results
		SI-12 Information Management and Retention SI-12 (3) Information Management and Retention | Information Disposal	
8	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies.	AT-5 Literacy Training and Awareness AT-3 Role-based Training PL-4 Rules of Behavior	**Exceptions noted.** **See Finding #1 above.**
9	**42 U.S.C § 2000ee-2, Privacy and Data Protection Policies and Procedures** Ensure compliance with the agency's established privacy and data protection policies. **OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Section I Risk Management Framework** 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 PM-31 Continuous Monitoring Strategy	**No exceptions noted.**
10	**Privacy Act of 1974, 5 U.S.C. Section 552a** 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 SA-8 (33) Security and Privacy Engineering Principles | Minimization	**No exceptions noted.**

Audit of FHFA's 2023 Privacy Program

#	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 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. **OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-F** 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.	PM-5 (1) System Inventory | Inventory of Personally Identifiable Information SI-12 (1) Information Management and Retention | Limit Personally Identifiable Information Elements	
11	**Privacy Act of 1974, 5 U.S.C. Section 552a** 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** Post privacy policies on agency Web sites used by the public. **OMB Circular No. A-130, Managing Information as a Strategic Resource, Section 5 Policy, Subsection F Privacy and Information Security, 1-J** 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** Privacy Act System of Records Notices are published, revised, and rescinded, as required.	PT-5 (2) Privacy Notice | Privacy Act Statements PT-6 System of Records Notices	**No exceptions noted.**

Audit of FHFA's 2023 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control(s)	Results
14	**OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix I, Section 4 Specific Requirements, E-8** Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization. **OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix I, Section 4 Specific Requirements, E-9** 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.**

STATUS OF PRIOR RECOMMENDATIONS

The table below (**Table 4)** summarizes the status of our follow up related to the status of the open prior privacy-related recommendations.[31]

Table 4: Status of Prior Recommendations

Report Number / Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
AUD 2021-011, Finding # 1	We recommend that FHFA management: 1. Update the Privacy Impact Analysis (PIAs) using the PIA Template for Affordable Housing Project (AHP), Federal Human Resources (FHR) Navigator, and Suspended Counter Party System (SCP).	We found that the prior year recommendation has been resolved. Management updated the PIAs using the PIA Template for AHP, FHR Navigator, and SCP.	**Closed.**
	We recommend that FHFA management: 2. Ensure PIAs are conducted timely using the PIA Template in accordance with the *FHFA Privacy Program Plan* (i.e., before a new system is developed, after a significant change to a system, or	We found that the prior year recommendation has been resolved. FHFA Privacy Office updated the *FHFA Privacy Program Plan* and removed the requirement to review existing PIAs every three years. FHFA created a Continuous Monitoring schedule, scheduling reviews of PIAs.	**Closed.**

[31] See footnote 5.

Audit of FHFA's 2023 Privacy Program

Report Number / Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	within three years of the PIA).		
AUD 2021-011, Finding # 2	We recommend that FHFA management: 3. Update the *Privacy Continuous Monitoring Strategy* to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular No. A-130.	We found that the prior year recommendation has not been resolved. We noted that the FHFA *Privacy Continuous Monitoring Strategy*, Revision 2.0 (April 29, 2022), described the control assessments conducted by the Information Security Continuous Monitoring team. However, it did not include the FHFA Privacy Office's current privacy control assessment processes such as the Privacy Office's three-year PIA review cycle and their workplan, detailing privacy control reviews and PIA reviews.	**Open**. See finding # 4.
AUD 2021-011, Finding # 3	We recommend that FHFA management: 4. Develop and implement privacy control assessment plans that include all required elements.	We found that the prior year recommendation has been resolved. FHFA *Privacy Control Assessment Plan for Privacy Program Plan* (May 2, 2022) includes all required elements.	**Closed.**
	We recommend that FHFA management: 5. Ensure privacy control assessments are performed for all systems that collect personal identifiable information (PII).	We found that the prior year recommendation has been resolved. Privacy control assessments were performed for systems that collect PII.	**Closed.**

MANAGEMENTS' COMMENTS

FHFA-OIG's Management Comments

(1 page follows)

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

July 24, 2023

TO: Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

FROM: Dayle Elieson, Chief Counsel DAYLE ELIESON Digitally signed by DAYLE ELIESON Date: 2023.07.24 15:39:57 -04'00'

SUBJECT: Management Response to Draft Performance Audit of FHFA-OIG's Privacy Program and Practices

Thank you for the opportunity to review the draft audit report by CliftonLarsonAllen LLP of FHFA's and FHFA-OIG's implementation of privacy and data protection programs, policies, and practices. The draft report contains the following recommendation with respect to FHFA-OIG:

Recommendation 1: FHFA-OIG's Chief Counsel update the FHFA-OIG Privacy Program Plan to include procedures to verify personnel's completion of annual role-based privacy training. Procedures should include periodic progress checks and follow-up with personnel to ensure timely training completion.

Management Response: FHFA-OIG agrees with Recommendation 1. FHFA-OIG will finalize the update of its Privacy Program Plan, to include specific steps to ensure and verify completion of annual role-based privacy training by all personnel required to complete the training, by September 30, 2023.

If you have any questions, please contact Gregg Schwind at (202) 730-4933 or by email at gregg.schwind@fhfaoig.gov.

Audit of FHFA's 2023 Privacy Program

FHFA's Management Comments

(3 pages follows)

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

FROM: Tasha Cooper, Senior Agency Official for Privacy TASHA COOPER Digitally signed by TASHA COOPER Date: 2023.07.26 15:06:35 -04'00'

SUBJECT: Draft Audit Report: Audit of the Federal Housing Finance Agency's Privacy Program, Fiscal Year 2023

DATE: July 26, 2023

Thank you for the opportunity to respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains five new recommendations and reaffirms one recommendation from the 2021 privacy audit. We are pleased that the audit concluded that collectively the Agency generally implemented comprehensive privacy and data protection policies, procedures, and practices consistent with legal and regulatory guidance.

This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the five recommendations (four new recommendations and one recommendation from the 2021 privacy audit) specific to FHFA in the Report. The Report also makes one recommendation (Recommendation 1) specific to the FHFA OIG, who will respond in a separate memorandum.

Recommendation 2: *Revise the FHFA Privacy Program Plan to document the frequency of review for existing PIAs in accordance with OMB Circular No. A-130.*

Management Response to Recommendation 2: FHFA agrees with the recommendation. FHFA's Privacy Office revised the FHFA Privacy Program Plan in July 2023 to document FHFA's review frequency for existing PIAs.

Recommendation 3*: In coordination with the System Owner and CISO, ensure that all required approval signatures are captured within the PIA and maintain a record of review for each PIA, as required by the FHFA Privacy Impact Assessment Guide.*

Management Response to Recommendation 3: FHFA agrees with the recommendation and implemented an electronic clearance process to ensure that all required approvals are captured on

the PIA. This process also serves as the record of review for each PIA. The PIA electronic clearance process is documented in the PIA Guide, which was updated in April 2023.

Recommendation 4: *Update the PIAs for the Everbridge Suite, the NMDB, and the OneStream XF to ensure PIAs accurately describe all security and privacy controls of the system and are approved by the required officials.*

Management Response to Recommendation 4: FHFA agrees with the recommendation and will update the Everbridge Suite, NMDB, and the OneStream XF PIAs to ensure that the PIAs accurately describe all security and privacy controls of the system and are approved by the required officials by November 30, 2023.

Recommendation 5: *In coordination with the originating office and the Office of General Counsel, obtain and review proposed rules, and determine if a PIA is required, in accordance with FHFA Policy No. 801, Official Documents Policy.*

Management Response to Recommendation 5: FHFA agrees with the recommendation. The Privacy Office emphasized its role in rulemaking during the Agency's 2023 annual privacy training. This training was required to be completed by FHFA staff by June 30, 2023. The Privacy Office is also working with the Office of General Counsel (OGC) to ensure that the Privacy Office is included in the electronic clearance process for all rulemakings before they are published in the Federal Register. FHFA will ensure that determinations of the need for a PIA in rulemakings are documented as required by the Official Documents Policy by November 30, 2023.

2021 Audit Recommendation (AUD-2021-011, Recommendation 3*): Update the Privacy Continuous Monitoring Strategy to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular No. A-130.*

Management Response to the 2021 Recommendation: As noted in the Report, the Privacy Office introduced a *Workplan* process to strengthen the privacy monitoring activities and remediation of self-identified operational deficiencies. However, the *Workplan* processes were not detailed in FHFA's *Privacy Continuous Monitoring Strategy* (April 29, 2022) when the audit testing was conducted. The Privacy Office updated the Privacy Continuous Monitoring Strategy to reference the privacy review tracking mechanism (currently referred to as the *Workplan*) in June 2023.

If you have questions, please contact me at (202) 649-3091 or by e-mail at Tasha.Cooper@fhfa.gov.

cc: Clinton Jones
Sean Dent
Ralph Mosios

John Major

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