Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's 2021 Privacy Program

Audit Report • AUD-2021-011 • August 11, 2021

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

August 11, 2021

TO: Sandra L. Thompson, Acting Director

FROM: Marla A. Freedman, Senior Audit Executive /s/

SUBJECT: Audit of the Federal Housing Finance Agency's 2021 Privacy Program

We are pleased to transmit the subject report.

42 U.S.C. § 2000ee-2, requires the Federal Housing Finance Agency (FHFA) to establish and implement comprehensive privacy and data protection procedures governing FHFA's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form related to employees and the public. Such procedures are to 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. 42 U.S.C. § 2000ee-2 also requires the Office of Inspector General (OIG) to periodically conduct a review of FHFA's implementation of this section and report the results of our review to the Congress.

We contracted with CliftonLarsonAllen LLP (CLA) to conduct a performance audit to meet our reporting requirement under 42 U.S.C. § 2000ee-2. The contract required that the audit be conducted in accordance with generally accepted government auditing standards.

Based on its audit work, CLA concluded that FHFA had generally 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, consistent with legal and regulatory guidance. CLA found that although FHFA generally implemented comprehensive privacy and data protection policies and procedures, its implementation of certain privacy requirements was not fully achieved. CLA noted weaknesses in privacy impact assessments, privacy continuous monitoring strategy, privacy control assessment plans, and maintenance of privacy policies and procedures. As a result, CLA made five recommendations to assist FHFA in strengthening its privacy program.

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 FHFA's compliance with 42 U.S.C. § 2000ee-2 and the applicable privacy controls tested by CLA. CLA is responsible for the attached auditor's report dated August 4, 2021, 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 auditor's report, FHFA management agreed with the five recommendations made in the report and outlined its plans to address each. CLA considers FHFA's planned corrective actions to meet the intent of its recommendations.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Privacy Program
Fiscal Year 2021

Audit of the Federal Housing Finance Agency's 2021 Privacy Program

August 4, 2021

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

August 4, 2021

The Honorable Phyllis K. Fong
Acting Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Acting Inspector General Fong:

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

We have reviewed FHFA's response to a draft of this report and have included our evaluation of management's comments within this final report. FHFA's comments are included in Appendix V.

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

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Acting Inspector General
Federal Housing Finance Agency

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Federal Housing Finance Agency's (FHFA or Agency) 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 the audit was to assess FHFA's implementation of its privacy program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether FHFA 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, consistent with legal and regulatory guidance.

The audit included tests of the implementation of federal privacy laws, regulations, standards, and FHFA privacy policy and procedures. These privacy requirements were mapped to applicable privacy controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, *Privacy Controls Catalog*. NIST's *Privacy 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, 42 U.S.C. § 2000ee-2, 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 12 systems that collected personally identifiable information (PII).

The audit also included evaluating whether FHFA took corrective actions to address privacy-related findings and recommendations in FHFA-OIG Audit Report AUD-2019-009, *Audit of the Federal Housing Finance Agency's 2019 Privacy Program*, dated August 28, 2019, and FHFA-OIG Report AUD-2021-001, *Audit of the Federal Housing Finance Agency's Information Security Program, Fiscal Year 2020*, dated October 20, 2020.

Audit fieldwork covered FHFA's headquarters located in Washington DC, from March 2021 to July 2021.

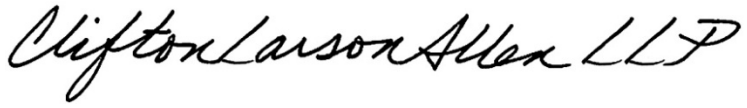
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We concluded that FHFA had generally 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, consistent with legal and regulatory guidance. However, while the Agency generally implemented comprehensive privacy and data protection policies and procedures, FHFA's implementation of certain privacy requirements was not fully achieved. We noted weaknesses in privacy impact assessments, privacy continuous monitoring strategy, privacy control assessment plans,

and maintenance of privacy policies and procedures. As a result, we made five recommendations to assist FHFA in strengthening its privacy program.

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

CliftonLarsonAllen LLP



Arlington, Virginia
August 4, 2021

Table of Contents

EXECUTIVE SUMMARY

The Federal Housing Finance Agency (FHFA) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit to review FHFA's implementation of its privacy program 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 (IG) periodically review their respective agencies' privacy programs.

The objective of this performance audit was to assess FHFA's implementation of its privacy program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether FHFA 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, 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-2019-009, *Audit of the Federal Housing Finance Agency's 2019 Privacy Program*, dated August 28, 2019, and FHFA-OIG Report AUD-2021-001*, Audit of the Federal Housing Finance Agency's Information Security Program, Fiscal Year 2020*, dated October 20, 2020.

The audit included tests of the implementation of federal privacy laws, regulations, standards, and FHFA privacy policy and procedures. These privacy requirements were mapped to applicable privacy controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, *Privacy Controls Catalog*.[1] The NIST *Privacy 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, 42 U.S.C. § 2000ee-2, 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[2] FHFA systems from total population of 12 systems that collected personally identifiable information (PII).

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.

[1] See Appendix III for mapping of controls.

[2] We sampled the following FHFA Privacy Systems: Affordable Housing Project, Federal Human Resources Navigator, and Suspended Counterparty System.

Summary of Results

Progress Since 2019

An audit of FHFA's privacy program was conducted in 2019[3] resulting in 11 recommendations for FHFA to strengthen its privacy program and one remaining open recommendation from 2017.[4] CLA followed up on the 2019 privacy audit recommendations during the fiscal year (FY) 2020 Federal Information Security Modernization Act (FISMA) audit,[5] and noted that FHFA took corrective actions to address and close 9 of the 11 recommendations in 2020. Additionally, the FY 2020 FISMA audit included one new privacy-related recommendation.

As a result, during 2021, there were four remaining open privacy-related recommendations (one open recommendation from the 2017 Privacy Audit, two open recommendations from the 2019 Privacy Audit, and one open recommendation from the FY 2020 FISMA audit). We found that FHFA took corrective actions to address one of those recommendations, and we consider the recommendation to be closed. Corrective action is in progress on the other recommendations. Refer to Appendix IV for a detailed description of the status of each recommendation.

Current Status

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

- Designating a Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer (CPO) with responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program.
- Documenting and maintaining current System of Records Notices (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 PII in accordance with Federal Information Processing Standards (FIPS).
- 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 and procedures, FHFA's implementation of certain privacy and data protection requirements was not fully achieved. As a result, we noted weaknesses in FHFA's privacy procedures and practices (**Table 1**) and made five recommendations to assist FHFA in strengthening its privacy program.

[3] FHFA-OIG Audit Report AUD-2019-009, *Audit of the Federal Housing Finance Agency's 2019 Privacy Program*, dated August 28, 2019.

[4] FHFA-OIG Audit Report AUD-2017-007, *Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program*, dated August 30, 2017.

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

Table 1: Summary of Findings and Recommendations

Privacy Program Weakness	Recommendations
1. Privacy Impact Assessments (PIA)	**Recommendation 1:** Update the PIAs using the PIA Template for Affordable Housing Project (AHP), Federal Human Resources Navigator (FHR Navigator), and Suspended Counterparty System (SCP). **Recommendation 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 within three years of the PIA).
2. Privacy Continuous Monitoring Strategy	**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 A-130.
3. Privacy Control Assessments	**Recommendation 4**: Develop and implement Privacy Control Assessment plans, that include all required elements. **Recommendation 5:** Ensure Privacy Control Assessments are performed for all systems that collect PII.

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

AUDIT FINDINGS

1. FHFA Needs to Improve Its Privacy Impact Assessment Process

Privacy risk management processes operate across the life cycles of all mission and business processes that collect, use, maintain, share, or dispose of PII. Privacy Threshold Analysis (PTA) and PIAs are common tools used for managing privacy risk. A PTA is a screening tool used to identify initial privacy requirements for information technology systems and to determine if a PIA is required for a system. PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. A PIA is both a process and a document of that process.

FHFA PIAs were not updated within the last three years as required by the *FHFA Privacy Program Plan* for the following three systems[6] selected for testing, that collect, use, maintain, and protect PII:

- AHP – The last PIA was dated May 2016.
- FHR Navigator – The last PIA was dated May 2010.
- SCP – The last PIA was dated December 2017.

The FHFA SAOP stated that FHFA did not update the PIAs since there were no significant changes that FHFA management believed would necessitate updates to the PIAs.

FHFA Privacy Program Plan, dated October 2019, states that:

> System of Records Owners, System Owners, and Information System Security Officers must conduct PIAs using the PIA Template before developing a new system, and thereafter if making a significant change to a system - when the system undergoes a security authorization and the new PTA shows additional privacy risks **-** or within three years after the most recent PIA.

Failure to 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.

We recommend that FHFA management:

> ***Recommendation 1:*** *Update the PIAs using the PIA Template for AHP, FHR Navigator, and SCP.*
>
> ***Recommendation 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 within three years of the PIA).*

2. FHFA Needs to Update Its Privacy Continuous Monitoring Strategy

FHFA's *Privacy Continuous Monitoring Strategy*, dated September 2020, stated that:

> FHFA performs ongoing control assessments in accordance with the Information Security Continuous Monitoring (ISCM) Ongoing Assessment Schedule

[6] See Appendix II, Table 2 for a description of each in-scope system.

> 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.

FHFA's *Privacy Continuous Monitoring Strategy* did not accurately describe FHFA's privacy control monitoring process. Specifically, the Strategy stated that privacy control assessments were included in the ISCM process. However, in practice, the scheduling, testing, and reporting of privacy controls were performed separately, outside of the ISCM process, by the SAOP.

The FHFA SAOP acknowledged that the FHFA's *Privacy Continuous Monitoring Strategy* did not accurately reflect current privacy control assessment practices, and stated that the strategy is under review.

OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix II, Section I Risk Management Framework, requires that the SAOP develops and maintains a privacy continuous monitoring (PCM) strategy and PCM program to maintain ongoing awareness of privacy risks.

Under the control environment component of internal control and the underlying principle of establish structure, responsibility, and authority in the *Standards for Internal Control in the Federal Government* (Green Book) published by the Government Accountability Office (GAO),[7] management should establish an organizational structure, assign responsibility, and delegate authority to achieve the Agency's objectives. Paragraph 3.10 of the Green Book states:

> Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

Failure to accurately describe the privacy control assessment process in the FHFA's *Privacy Continuous Monitoring Strategy* increases the risk that privacy control assessments and monitoring of controls will not be performed timely or adequately to address privacy risks.

We recommend that FHFA management:

> ***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 A-130.*

3. FHFA Needs to Improve Its Privacy Control Assessment Plans

Privacy control assessment plans were not documented in accordance with OMB and NIST requirements. Specifically, we noted the following:

[7] See GAO-14-704G (September 2014)

- We found that FHFA's privacy control assessment plans for two systems, FHR Navigator and SCP, did not contain all the required elements. Specifically, FHFA did not document the required elements of objectives and type of assessment in its plans. Additionally, the required element of roles and responsibilities were documented in the *FHFA Privacy Program Plan*, and the required element of assessment procedures were documented in email correspondence.
- For one out of three systems selected for testing, AHP, FHFA did not develop a privacy control assessment plan nor perform a privacy control assessment although the system collects PII.

The FHFA SAOP acknowledged that detailed privacy control assessment plans were not developed and documented for each system. According to the FHFA SAOP, a privacy control assessment was not conducted for AHP, as FHFA management believed it was unnecessary because they thought privacy control assessments were only supposed to be done for Privacy Act systems of records,[8] and not other systems that collected PII. However, the requirements of NIST SP 800-53, Appendix J, applies to all PII systems.

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

TASK A-2 Develop, review, and approve plans to assess implemented controls.

> Security and privacy assessment plans are developed by control assessors based on the implementation information contained in security and privacy plans, program management control documentation, and common control documentation.…An integrated assessment plan delineates roles and responsibilities for control assessment. Assessment plans also provide the objectives for control assessments and specific assessment procedures for each control. Assessment plans reflect the type of assessment the organization is conducting, including for example: developmental testing and evaluation; independent verification and validation; audits, including supply chain; assessments supporting system and common control authorization or reauthorization; program management control assessments; continuous monitoring; and assessments conducted after remediation actions.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Appendix J, provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII.

OMB Circular A-130, *Managing Information as a Strategic Resource,* dated July 28, 2016, Appendix II, Section I Risk Management Framework, requires that the SAOP develops and maintains a PCM strategy and PCM program to maintain ongoing awareness of privacy risks. This includes conducting privacy control assessments to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manages privacy risks.

[8] The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

Without comprehensive privacy control assessment plans documented, there may be an increased risk that FHFA may not be able to determine the extent to which the controls are operating effectively or as intended, are sufficient to ensure compliance with applicable privacy requirements, and are producing the desired outcome. As a result, FHFA may not be aware of privacy program risks, potentially increasing the possibility of PII being mismanaged.

We recommend that FHFA management:

> ***Recommendation 4****: Develop and implement privacy control assessment plans that include all required elements.*
>
> ***Recommendation 5:*** *Ensure privacy control assessments are performed for all systems that collect PII.*

EVALUATION OF MANAGEMENT COMMENTS

In response to a draft of this report, FHFA agreed with all five recommendations made in this report and outlined its plans to address each recommendation. We consider FHFA's planned corrective actions to meet the intent of our recommendations. FHFA's comments are included in Appendix V.

BACKGROUND

Agency Overview

Established by the Housing and Economic Recovery Act of 2008, Public Law 110-289, FHFA is an independent Federal agency with a Director appointed by the President and confirmed by the United States Senate. The agency's mission is to provide effective supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac, the 11 Federal Home Loan Banks (FHLBanks), and the FHLBanks' fiscal agent, the Office of Finance. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the FHLBanks.

FHFA's Privacy Program Overview

FHFA's privacy program is documented primarily in the *FHFA Privacy Program Plan*, and is supplemented by privacy and security policies and procedures. The *FHFA Privacy Program Plan* requires System of Records Owners, System Owners, and Information System Security Officers to conduct PIAs before developing a new system, and thereafter if making a significant change to a system and the new PTA shows additional privacy risks, or within three years after the most recent PIA.

While privacy is a key responsibility for all FHFA employees and contractors, FHFA has designated and assigned key roles and responsibilities to the following personnel and offices:

- The SAOP/CPO is responsible for implementation of FHFA's privacy program.
- The Privacy Office is responsible for day-to-day privacy activities.
- The Chief Information Security Officer is responsible for developing and implementing an organization-wide information security program.
- The Office of the General Counsel is responsible for providing legal advice on privacy related matters including systems of records notices and proposed rules.
- Program Managers and Information and System Owners are responsible for ensuring the privacy and security of the PII that their programs and/or information systems collect, use, disseminate, and maintain, and for complying with federal privacy laws, regulations, policies and guidelines.

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 CPO 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 A-130, *Managing Information as a Strategic Resource*

OMB Circular A-130, Appendix II, *Responsibilities for Managing Personally Identifiable Information*, dated 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST SP 800-53, Revision 4, Appendix J, *Privacy Control Catalog*, provides a structured set of privacy controls, based on best practices, that help organizations comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances.

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

Objective

The objective of the audit was to assess FHFA's implementation of its privacy program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether FHFA 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, consistent with legal and regulatory guidance.

Scope

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 scope of this audit included assessing FHFA's compliance with privacy and data protection requirements in accordance with law, regulation, and policy, covering the period from August 29, 2019 through March 31, 2021.[9] FHFA's privacy program was 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 FHFA's compliance with federal privacy laws, regulations, standards, and FHFA privacy policy and procedures. These privacy requirements were mapped to applicable privacy controls listed under NIST SP 800-53, Revision 4, Appendix J, *Privacy Controls Catalog*.[10] The NIST *Privacy 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, 42 U.S.C. § 2000ee-2, and OMB memoranda. We assessed FHFA'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

[9] The scope of this audit covered the period since the FHFA-OIG Audit Report AUD-2019-009, *Audit of the Federal Housing Finance Agency's 2019 Privacy Program*, issued August 28, 2019.

[10] Appendix J: Privacy Controls Catalog is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

See Appendix III for an overview of federal privacy criteria evaluated. In addition, the audit included an assessment of the implementation of federal privacy requirements for a sample of three information systems from the total population of 12 FHFA systems that collected PII (**Table 2**).

Table 2: Description of Systems Selected for Testing

Privacy System Name	Description
AHP	AHP captures information pertaining to AHP, homeownership set-aside program, Community Investment Program (CIP), and Community Investment Cash Advance (CICA) program via an AHP submission. The FHLBanks submit files via an Extranet AHP upload application.
FHR Navigator	FHR Navigator is an integrated web-based enterprise system that automates federal HR within a single platform. It is designed to automate federal HR administrative activities; manage different HR function tasks through an integrated system; accelerate and streamline typical HR processing steps, and support new government-wide hiring and workforce planning initiatives; and support services that HR offices deliver to employees, such as providing benefits administration services counseling and preparing retirement packages. The FHR Navigator system is for internal use only and does not post publicly accessible information.
SCP	SCP was established to help address the risk to Fannie Mae, Freddie Mac, and the FHLBanks ("the regulated entities") presented by individuals and entities with a history of fraud or other financial misconduct. SCP records may include name, address, Social Security number, date of birth, professional license number or other identifying information, type of sanction, date of sanction, court or agency responsible, description of misconduct, affiliate information (name, address, professional license number or other identifying information, description of how the affiliate is related to the subject), online profile or account information, and information pertaining to criminal prosecutions, civil actions, enforcement proceedings, and investigations resulting from or relating to fraud or suspected fraud or other financial misconduct. Such records may also include information on individuals: (a) who have been referred to FHFA for possible suspension; (b) who are currently or have been engaged in a covered transaction with a regulated entity within three years of when the regulated entity becomes aware of the covered misconduct; or (c) who are affiliates of such persons or institutions.

The audit also included an evaluation of whether FHFA took corrective action to address open privacy-related findings and recommendations from the 2019 Privacy Audit Report and the FY 2020 FISMA report.[11]

Audit fieldwork covered FHFA's Headquarters located in Washington DC, from March 2021 to July 2021.

The control environment component of internal control is significant to FHFA's operations. The underlying principle that management should establish an organizational structure, assign responsibility, and delegate authority is essential for FHFA to achieve its objectives. Our work did not include an assessment of the sufficiency of internal control over financial reporting 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 FHFA on or before August 4, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to August 4, 2021.

Methodology

To determine if FHFA implemented effective privacy and data protection policies and procedures, we performed the following tasks:

- Interviewed key personnel and reviewed legal and regulatory privacy requirements.
- Reviewed documentation related to FHFA's privacy program, such as the *FHFA 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.
- Tested privacy-related processes to determine if FHFA implemented federal privacy requirements (See Appendix III).
- 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 FHFA policies and federal criteria, including, but not limited to, the following:

- The Privacy Act of 1974, 5 U.S.C. Section 552a
- 42 U.S.C. § 2000ee–2, *Privacy and Data Protection Policies and Procedures*
- Section 208 of the E-Government Act of 2002
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- 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 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*

[11] Ibid. footnotes 3 and 5.

- FHFA privacy-related policies and procedures, including but not limited to: FHFA's *Privacy Continuous Monitoring Strategy*, dated September 2020 and *FHFA Privacy Program Plan,* dated October 2019

CLA selected the three systems **(Table 2)** from the total population of 12 FHFA systems that collected PII. The three systems were selected based on risk. Specifically, three moderate categorized systems[12] that were not recently assessed during prior audits were selected from the total population of FHFA systems that collected PII.

In testing for the adequacy and effectiveness of the privacy program controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk, and the significance or criticality of the specific items in achieving the related control objectives was considered. 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.

[12] Security categorizations are determined by federal agencies using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 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 notes the federal privacy requirements we reviewed for FHFA's privacy program, mapped to applicable privacy controls listed under NIST SP 800-53, Revision 4, Appendix J, *Privacy Controls Catalog*.[13]

We tested the following entity and system-level federal privacy requirements to conclude on FHFA's privacy program. 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 A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information** Establish and maintain a comprehensive privacy program that (1) ensures compliance with applicable privacy requirements, (2) develops and evaluates privacy policy, and (3) manages privacy risks.	AR-1 Governance and Privacy Program	**Exceptions noted.** **See Appendix IV – prior year finding - AUD 2021-001, Recommendation #4**
	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.**

[13] Appendix J: Privacy Controls Catalog is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

#	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.		**Exceptions noted.** **See Appendix IV – prior year finding - AUD 2019-009, Recommendation #5**
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.	AR-7 Privacy-enhanced System Design and Development	**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.	AR-7 Privacy-enhanced System Design and Development	**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].	SE-1 Inventory of Personally Identifiable Information AR-6 Privacy Reporting	**No exceptions noted.**
	OMB Circular 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 FIPS 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*.	SE-1 Inventory of Personally Identifiable Information	**No exceptions noted.**

#	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.	AR-2 Privacy Impact and Risk Assessment	**No exceptions noted.**
	Section 208 of the E-Government Act of 2002 Conduct PIAs of information technology and collections and, in general, make PIAs publicly available.	AR-2 Privacy Impact and Risk Assessment	**Exceptions noted.** **See Finding #1 above.**
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 552a of title 5, 11 internal controls, and other relevant matters.	AR-6 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.	DI-2 Data Integrity and Data Integrity Board DM-2 Data Retention and Disposal	**No exceptions noted.**
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.	AR-5 Privacy Awareness and Training	**No exceptions noted.**
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 A-130, Managing Information as a Strategic Resource, Appendix II** Ensure the SAOP develops and maintains a PCM strategy and PCM 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,	AR-4 Privacy Auditing and Monitoring	**Exceptions noted.** **See Findings #2 and #3 above.**

#	Federal Criteria	NIST SP 800-53 Control (s)	Results
	operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manages privacy risks**.**		
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. **OMB Circular A-130, Managing Information as a Strategic Resource, Appendix II** 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.	AP-1 Authority to Collect DM-1 Minimization of Personally Identifiable Information	**No exceptions noted.**
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.	AR-8 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.	TR-3 Dissemination of Privacy Program Information	**No exceptions noted.**
13	**OMB Circular A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information** Publish, revise, and rescind Privacy Act system of records notices, as required.	TR-2 System of Records Notices and Privacy Act Statements	**No exceptions noted.**
14	**OMB Circular A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information** Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization. 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.	CA-6 Security Authorization	**Exceptions noted.** **See Appendix IV – prior year finding - AUD 2019-009, Recommendation 6**

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of our follow up related to the status of the open prior privacy-related recommendations.[14]

Report Number / Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
AUD 2017-007, Finding #1	We recommend that FHFA Privacy Office: 3. Establish, implement, and train end users to apply naming conventions to files and folders containing PII.	We found that FHFA and its Records and Information Management Group documented and finalized the agency's Controlled Unclassified Information (CUI) policy to educate end-users to naming conventions to files and folders containing PII.	**Closed**
AUD 2019-009, Finding #3	We recommend that FHFA Privacy Office: 5. Determine privacy controls that are information system-specific, and/or hybrid controls.	We found that the prior year recommendation has not been resolved. FHFA has not designated whether each privacy control is a program management, common, system-specific, or hybrid control. Specifically, neither, the *FHFA Program Plan for Privacy,* nor system security plans (SSPs) for AHP, FHR Navigator, and SCP designated which privacy control is a program management, common, system-specific, or hybrid control.	**Open** We note that FHFA disagreed with this recommendation. However, FHFA committed to a course of action that met the intent of the recommendation. That action is to be completed within one year of the publication of Revision 5 to NIST SP 800-53.

[14] Ibid. footnotes 3, 4, and 5.

Report Number / Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
			Revision 5, was published December 10, 2020.
	We recommend that FHFA Privacy Office: 6. Document privacy controls within each system's [System Security Plan] or system-specific privacy plan, clearly identifying whether controls are program level, common, information system-specific, or hybrid.	We found that the prior year recommendation has not been resolved. Privacy controls were not documented within the SSPs for the FHFA information systems selected for testing: • AHP • FHR Navigator • SCP	**Open** We note that FHFA disagreed with this recommendation. However, FHFA committed to a course of action that met the intent of the recommendation. That action is to be completed within one year of the publication of Revision 5 to NIST SP 800-53. Revision 5, was published December 10, 2020.
AUD 2021-001, Finding #4	We recommend that FHFA management: 4. Ensure privacy-related policies and procedures are reviewed and kept up-to-date at least on a	We found that the prior year recommendation has not been resolved. The following policies and procedures have not been updated in accordance with NIST SP 800-53 Revision 4: • *FHFA Policy 301 Use and Protection of PII Policy.*	**Open** We note that FHFA committed to complete its corrective actions to this

Report Number / Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	biennial basis in accordance with NIST SP 800-53, Revision 4. The review should be documented and annotated in the version history for each document to summarize any updates and/or no updates required, as applicable.	• *Procedures for Monitoring FHFA's Website for Compliance with Privacy and Social Media Policies.*	recommendation by August 31, 2021.

FHFA's MANAGEMENT COMMENTS

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

FROM: Tasha Cooper, Senior Agency Official for Privacy

Cooper, Tasha L. Digitally signed by Cooper, Tasha L. Date: 2021.07.23 16:44:58 -04'00'

Kevin Smith, Chief Information Officer

KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2021.07.22 15:36:58 -04'00'

SUBJECT: Draft Audit Report: Audit of the Federal Housing Finance Agency's 2021 Privacy Program

DATE: July 22, 2021

Thank you for the opportunity to respond to the above-referenced draft Office of Inspector General audit report (Report). This memorandum provides Federal Housing Finance Agency's (FHFA) management response to the Report's five recommendations.

Recommendation 1: Update the PIAs using the PIA Template for Affordable Housing Project (AHP), Federal Human Resources Navigator (FHR Navigator), and Suspended Counterparty System (SCP).

Management Response: FHFA agrees with Recommendation 1. FHFA will update the AHP, FHR Navigator, and SCP PIAs by July 29, 2022.

Recommendation 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 within three years of the PIA).

Management Response: FHFA agrees with Recommendation 2. FHFA will ensure that new PIAs are completed prior to a new system or a significant system change that is placed into production or update the existing PIA within 3 years of its implementation date by July 29, 2022.

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 A-130.

Management Response: FHFA agrees with Recommendation 3. FHFA will update the Update the *Privacy Continuous Monitoring Strategy* to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular A-130 by July 29, 2022.

Recommendation 4: Develop and implement standardized Privacy Control Assessment plans, that include all required elements.

Management Response: FHFA agrees with Recommendation 4. FHFA will develop and implement standardized Privacy Control Assessment plans, that include all required elements by July 29, 2022.

Recommendation 5: Ensure Privacy Control Assessments are performed for all systems that collect PII.

Management Response: FHFA agrees with Recommendation 5. FHFA will ensure that Privacy Control Assessments are performed or updated for all systems that collect PII by July 29, 2022.

If you have any questions, please feel free to contact Stuart Levy at (202) 649-3610 or by e-mail at Stuart.Levy@fhfa.gov.

CC: Katrina 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