

Federal Housing Finance Agency
Office of Inspector General



Audit of the Federal Housing Finance Agency's 2019 Privacy Program

Audit Report • AUD-2019-009 • August 28, 2019



OFFICE OF INSPECTOR GENERAL

Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

August 28, 2019

TO: Dr. Mark A. Calabria, Director

FROM: Marla A. Freedman, Deputy Inspector General for Audits /s/

SUBJECT: Audit of the Federal Housing Finance Agency's 2019 Privacy Program

We are pleased to transmit the subject report.

42 U.S.C. § 2000ee-2, requires FHFA to establish and implement comprehensive privacy and data protection procedures governing the agency'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 the independent certified public accounting firm of CliftonLarsonAllen (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 effective privacy and data protection policies and procedures in accordance with law, regulation, and policy. CLA found that although FHFA generally implemented an effective privacy program, its implementation of certain privacy requirements was not fully achieved. CLA noted weaknesses in the maintenance of privacy policies and procedures, privacy continuous monitoring, privacy control documentation, protection of information systems from unauthorized access to PII, privacy impact assessments, and privacy training. As a result, CLA made 11 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 22, 2019, 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 to 7 of the 11 audit recommendations and CLA concurred with management's response to those recommendations (i.e., management's corrective actions taken and planned with respect to recommendations 1 to 4 and 9 to 11). Although management disagreed with recommendations 5 and 6, management stated in its response that it planned to address the recommendations once certain National Institute of Standards and Technology guidance is updated. CLA determined, and we agreed, that management's response met the intent of the recommendations. We therefore consider these recommendations as agreed to by management, with implementation pending. Management also disagreed with recommendations 7 and 8, which called for FHFA to determine the feasibility of disabling inactive accounts for certain applications at a frequency that fits business needs, document that determination, and either implement automatic disabling of inactive accounts or compensating manual controls. However, CLA noted that FHFA management in its response had reached a decision with respect to the disabling of accounts at the application layer (deciding to rely on other controls instead); but had not formally documented this decision in accordance with National Institute of Standards and Technology guidance. We consider these two recommendations rejected and closed. Nevertheless, we encourage FHFA to formally document its decision in this regard, as recommended by CLA.

Report Distribution

Federal Housing Finance Agency

Director
Chief of Staff
Chief Operating Officer
Associate General Counsel and Senior Agency Official for Privacy
Chief Information Officer
Internal Controls and Audit Follow-up Manager

Office of Management and Budget

Budget Examiner

United States Senate

Chair and Ranking Member
Committee on Appropriations, Subcommittee on Transportation, Housing and Urban Development, and Related Agencies
Committee on Homeland Security and Governmental Affairs

U.S. House of Representatives

Chair and Ranking Member

Committee on Appropriations, Subcommittee on Transportation, Housing and Urban
Development, and Related Agencies

Committee on Oversight and Government Reform



**Audit of the
Federal Housing Finance Agency's
2019 Privacy Program**

August 22, 2019

Final Report



CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

August 22, 2019

The Honorable Laura S. Wertheimer
Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Inspector General Wertheimer:

CliftonLarsonAllen LLP (CLA) is pleased to present our Audit of the Federal Housing Finance Agency's 2019 Privacy Program Report, which details the results of our 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. 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 and appreciate the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

Sarah Mirzakhani, CISA
Principal



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 effective privacy and data protection policies and procedures.

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 listed under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 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 four FHFA systems from the total population of 11 systems that housed personally identifiable information (PII).

The audit also included evaluating whether FHFA took appropriate corrective actions to address the findings and recommendations in FHFA Office of Inspector General (FHFA OIG) Audit Report AUD-2017-007, *Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program*, issued August 30, 2017.

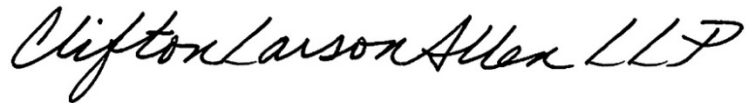
Audit fieldwork was performed at FHFA's headquarters in Washington, D.C., from March 27, 2019 to July 18, 2019.

Our audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. 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 effective privacy and data protection policies and procedures in accordance with law, regulation, and policy. Although FHFA generally implemented an effective privacy program, its implementation of certain privacy requirements was not fully achieved. We noted weaknesses in the maintenance of privacy policies and procedures, privacy continuous monitoring, privacy control documentation, protection of information systems from unauthorized access to PII, privacy impact assessments, and privacy training. As a result, we made 11 recommendations to assist FHFA in strengthening its privacy program.

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

CliftonLarsonAllen LLP

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The script is fluid and cursive, with the letters connected in a continuous line.

Arlington, Virginia
August 22, 2019

Audit of FHFA's 2019 Privacy Program

Table of Contents

EXECUTIVE SUMMARY	1
Summary of Results	2
 PRIVACY AUDIT FINDINGS	 4
1. FHFA Needs to Improve the Process for Maintaining Privacy Policies and Procedures	4
2. FHFA Needs to Strengthen Its Privacy Monitoring Program.....	4
3. FHFA Needs to Improve Its Privacy Control Documentation.....	6
4. FHFA Needs to Strengthen Protection of Information Systems from Unauthorized Access to Personally Identifiable Information	7
5. FHFA Needs to Improve Its Management of Privacy Impact Assessments	8
6. FHFA Needs to Strengthen Its Privacy Training Program	9
 EVALUATION OF MANAGEMENT COMMENTS.....	 11
 APPENDIX I – BACKGROUND.....	 15
APPENDIX II – OBJECTIVE, SCOPE AND METHODOLOGY	15
APPENDIX III – DETAILED TEST RESULTS	18
APPENDIX IV – STATUS OF PRIOR RECOMMENDATIONS	22
APPENDIX V – FHFA's MANAGEMENT RESPONSE.....	24

EXECUTIVE SUMMARY

The Federal Housing Finance Agency Office of Inspector General (FHFA OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit to assess the Federal Housing Finance Agency's (FHFA or Agency) 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 the audit was to assess FHFA's implementation of its privacy program in accordance with federal law, regulation, and policy. Specifically, the audit was 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. In addition, the audit included evaluating whether FHFA took corrective actions to address the findings and recommendations in FHFA OIG Audit Report AUD-2017-007, *Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program*, issued August 30, 2017.

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 listed under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, *Privacy Controls Catalog*.¹ 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 four² FHFA systems from total population of 11 systems that housed personally identifiable information (PII).

The audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. 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: General Support System (GSS), Correspondence Tracking Systems (CTS), Merit Central/Job Performance Plan (JPP), and FOIAExpress.

Audit of FHFA's 2019 Privacy Program

Summary of Results

Progress Since 2017

An audit of FHFA's Privacy Program was conducted in 2017 resulting in six recommendations for FHFA to strengthen its Privacy Program.³ Subsequently, FHFA took corrective actions to address and close five of those recommendations. Corrective action is in progress on the other recommendation. Refer to Appendix IV for a detailed description of the status of each recommendation.

Current Status

We concluded that FHFA had generally implemented effective privacy and data protection policies and procedures in accordance with law, regulation, and policy. Specifically, we noted that FHFA had effectively implemented the following privacy requirements:

- Designating a Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer (CPO) with agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program.
- Documenting and maintaining current System of Records Notices (SORNs).
- Conducting annual reporting 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 FHFA generally implemented an effective privacy program, its implementation of certain privacy requirements was not fully achieved. As a result, we noted weaknesses in the Agency's privacy policies and procedures, and practices (**Table 1**) and made 11 recommendations to assist FHFA in strengthening its privacy program.

Table 1: Summary of Findings and Recommendations

Privacy Program Weaknesses	Recommendation
1. Maintenance of privacy policies and procedures	Recommendation 1: Develop and implement a process to ensure that FHFA's Privacy Program Plan, and privacy-related policies and procedures are reviewed and kept up-to-date at least on a biennial basis in accordance with NIST SP 800-53, Revision 4. The review and updates should be recorded, such as in a version history for each document.
2. Privacy continuous monitoring	Recommendation 2: Develop a schedule and/or rotation plan to assess privacy controls as required by FHFA's Privacy Continuous Monitoring Strategy. Recommendation 3: Develop and implement a process to formally test privacy controls documented within the FHFA's Program Plan for Privacy Controls on at least an annual basis in

³ FHFA OIG Audit Report AUD-2017-007, *Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program*, issued August 30, 2017.

Audit of FHFA's 2019 Privacy Program

Privacy Program Weaknesses	Recommendation
	<p>accordance with the schedule and/or rotation to be developed as part of FHFA's Privacy Continuous Monitoring Strategy.</p> <p>Recommendation 4: Develop and implement a process to identify and review metrics to measure the effectiveness of privacy activities and compliance with privacy requirements as specified by OMB.</p>
3. Privacy control documentation	<p>Recommendation 5: Determine privacy controls that are information system-specific, and/or hybrid controls.</p> <p>Recommendation 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.</p>
4. Protection of information systems from unauthorized access to PII	<p>Recommendation 7: Determine the feasibility for automatically disabling inactive application accounts for [Correspondence Tracking System (CTS)] and [Merit Central/Job Performance Plan (JPP)] at a frequency that fits the business needs; and update applicable system policies and procedures, as necessary.</p> <p>Recommendation 8: Implement a control at the application layer to ensure inactive application accounts for CTS and Merit Central/JPP are disabled in accordance with the determined system frequency. If the application does not accommodate automatic disabling of inactive accounts, then consider implementing manual compensating controls (i.e., manually reviewing and disabling dormant accounts) to help mitigate the risk.</p>
5. Privacy Impact Assessments	<p>Recommendation 9: Review and update the Merit Central/JPP [Privacy Impact Assessment (PIA)] to ensure it accurately describes all PII collected by the system.</p> <p>Recommendation 10: Implement a process to ensure all of the Agency's PIAs are consistently updated and reviewed to include all types of PII a system collects, in accordance with FHFA Privacy Threshold Analysis and Privacy Impact Assessment Guide.</p>
6. Privacy Training Program	<p>Recommendation 11: Ensure all personnel whose responsibilities include access to PII complete annual privacy role-based training, whether via the planned web based application or by other means.</p>

The following section provides additional information on the findings identified. Detailed test results can be found in Appendix III.

AUDIT FINDINGS

1. FHFA Needs to Improve the Process for Maintaining Privacy Policies and Procedures

There was no documented evidence of at least a biennial review maintained for the following FHFA privacy plans, and privacy-related policies and procedures as required by the NIST:

- FHFA Program Plan for Privacy Controls
- FHFA Privacy Threshold Analysis (PTA) and PIA Assessment Guide
- Guidance on Accounting for Disclosures under the Privacy Act
- Guidance on Amending or Correcting Records in a SORN
- Procedures for Social Security Number (SSN) Collection
- SORN Procedures
- Teleworking and Information Security
- Use and Protection of PII

The FHFA SAOP stated that documentation of reviews and/or updates made to the privacy plan, policies, or procedures was not maintained.

NIST SP 800-53, Revision 4, Privacy Control AR-1 - Governance and Privacy Program Control, requires organizations to update their privacy plan, policies and procedures on an organizationally defined frequency, at least biennially.

Without an up-to-date privacy plan, and privacy-related policies and procedures, current privacy control requirements may not be accurately reflected, disseminated, and implemented. Moreover, employees and contractors may be performing tasks without clear direction, potentially increasing the risk that PII may be mishandled which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

To assist FHFA in strengthening the governance and privacy program, we recommend the FHFA Senior Agency Official for Privacy:

Recommendation 1: Develop and implement a process to ensure that FHFA's Privacy Program Plan, and privacy-related policies and procedures are reviewed and kept up-to-date at least on a biennial basis in accordance with NIST SP 800-53, Revision 4. The review and updates should be recorded, such as in a version history for each document.

2. FHFA Needs to Strengthen Its Privacy Continuous Monitoring Program

FHFA did not test and evaluate the effectiveness of privacy policies, procedures, and practices on at least an annual basis as required by the OMB. Specifically, we noted the following:

- The most recent privacy control assessment was conducted in July 2014. This assessment included privacy controls documented in FHFA's Program Plan for Privacy Controls.

Audit of FHFA's 2019 Privacy Program

- Privacy control assessments were not performed as required by the *FHFA's Privacy Continuous Monitoring Strategy* for the following systems selected for testing:
 - FHFA General Support System (GSS)
 - Correspondence Tracking System (CTS)
 - Merit Central/Job Performance Plan (JPP)
 - FOIAXpress

Additionally, FHFA has not identified and reviewed metrics to measure the effectiveness of privacy activities and compliance with privacy requirements as specified by OMB.

The FHFA SAOP stated that a schedule and/or rotation plan had not been established to assess privacy controls as required by *FHFA's Privacy Continuous Monitoring Strategy*. FHFA relied on testing a portion of security controls that may be related to privacy (e.g., AC-2 Account Management) on an annual basis. In addition, the FHFA SAOP further stated that metrics have not been developed because of competing priorities in the privacy office which took precedent over the metrics.

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. This includes conducting privacy control assessments, and 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. Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually.

FHFA's Privacy Continuous Monitoring Strategy requires that FHFA perform ongoing control assessments in accordance with the Information System Continuous Monitoring (ISCM) Ongoing Assessment Schedule maintained by the ISCM Team. Privacy controls are to be included in the ISCM Ongoing Assessment Schedule. The schedule is required to 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. This includes assessing some controls at more frequent intervals than others, based on their volatility of other factors.

Without periodically assessing the agency's privacy controls and identifying and measuring performance metrics, 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.

To assist FHFA in strengthening the privacy continuous monitoring program, we recommend the FHFA Senior Agency Official for Privacy:

Recommendation 2: *Develop a schedule and/or rotation plan to assess privacy controls as required by FHFA's Privacy Continuous Monitoring Strategy.*

Recommendation 3: *Develop and implement a process to formally test privacy controls documented within the FHFA's Program Plan for Privacy Controls on at least an annual*

Audit of FHFA's 2019 Privacy Program

basis in accordance with the schedule and/or rotation to be developed as part of FHFA's Privacy Continuous Monitoring Strategy.

Recommendation 4: *Develop and implement a process to identify and review metrics to measure the effectiveness of privacy activities and compliance with privacy requirements as specified by OMB.*

3. FHFA Needs to Improve Its Privacy Control Documentation

The *FHFA Program Plan for Privacy* identifies all privacy controls at the organizational level even though certain privacy controls should be documented at the information system level. Examples of system-specific and/or hybrid privacy controls that are not identified in the *FHFA Program Plan for Privacy* include but are not limited to: AR-2: Privacy Impact and Risk Assessment related to conducting PIAs for information systems that pose a privacy risk; AR-7: Privacy-Enhanced System Design and Development which addresses designing the information system to support privacy by automating privacy controls; DM-3: Minimization of PII Used in Testing, Training and Research related to the use of PII for testing new applications or information systems prior to deployment; or DM-2: Data Retention and Disposal which addresses the methods used to ensure secure deletion or destruction of PII.

Specifically, privacy controls were not documented within the System Security Plans (SSPs) for the following FHFA information systems selected for testing:

- FHFA GSS
- CTS
- Merit Central/JPP
- FOIAXpress

The FHFA SAOP stated that they applied the guidance in NIST SP 800-53 Revision 4 regarding implementation of the privacy control families at either the organization or system-specific level, and made the determination all privacy controls for the Agency are at the organization level.

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires that the SAOP:

- Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency.
- 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.

OMB A-130 defines 'Authorization package' as the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

Specificity of controls documented at the system and/or hybrid level provides clarity and direction for System Owners (SOs) and Information System Security Officers (ISSOs) to implement privacy controls where they have significant responsibilities, or in the automation of privacy controls within

Audit of FHFA's 2019 Privacy Program

the information system. Additionally, this specificity would provide details regarding individual system distinctions. A lack of documentation of privacy controls at the information system level increases the risk of key privacy control responsibilities going unfulfilled, thus increasing the risk of PII being mismanaged.

In addition, if SSPs do not document system-specific distinctions (e.g., specific automated controls, specific ISSO or SO responsibilities, etc.), the SAOP may not fully understand the distinctions of how system-specific and/or hybrid privacy controls are implemented for the information system. This could directly affect the decision making process when accepting the risk associated with the effectiveness of privacy controls as an authorizing official.

To assist the FHFA in improving its privacy control documentation, we recommend the FHFA Senior Agency Official for Privacy:

Recommendation 5: *Determine privacy controls that are information system-specific, and/or hybrid controls.*

Recommendation 6: *Document privacy controls within each system's SSP or system-specific privacy plan, clearly identifying whether controls are program level, common, information system-specific, or hybrid.*

4. FHFA Needs to Strengthen Protection of Information Systems from Unauthorized Access to PII

Two out of three information systems selected for testing, that house PII, did not have technical controls in place to automatically disable user accounts within the applications after a defined period of inactivity. These systems, CTS and Merit Central/JPP, authenticate via single sign-on with Active Directory.

The FHFA SAOP and an Agency information security specialist stated that management interpreted the definition of an information system in NIST SP 800-53 Revision 4, Access Control AC-2, Account Management, to only apply to the network and not the application. In addition, FHFA relied on disabling the network accounts at the Active Directory layer as a sufficient control. The SAOP also stated that users of these applications only need to access these systems a few times a year. Therefore, if they disabled users' application accounts after 35 days of inactivity, in accordance with FHFA GSS SSP, that would affect users' ability to readily access data when needed. Users would be required to contact the help desk to reactivate their disabled application accounts.

NIST SP 800-53, Revision 4, Control AC-2 Account Management, requires that organizations create, enable, modify, disable, and remove information system accounts in accordance with organization-defined procedures or conditions.

In addition, Control AC-2, Control Enhancement 3, Account Management | Disable Inactive Accounts, requires the information system to automatically disable inactive accounts after an organization-defined time period.

Single sign-on is a useful tool that allows users to login once and gain access to all systems in which they are authorized, without any additional login prompts. However, the convenience of this tool does not negate the agency's responsibilities for implementing and analyzing risk associated

Audit of FHFA's 2019 Privacy Program

with required controls at the application layer. Agencies must balance the convenience of that authentication method with the risks that accompany it, and formally document their controls and risk-based decisions (based on business need, mitigating controls, requirements with standards, and desired security posture).

There is a risk that active dormant application accounts (accounts that remain active after a defined period of inactivity) can be mishandled and misused, increasing the risk of unauthorized or improper access to PII and other sensitive agency data associated with the applications. Specifically, the applications house the following sensitive data:

- CTS captures information on the sender and the nature of the correspondence (e.g., name; property, home, and business addresses; e-mail address; telephone numbers; other personal and contact information, etc.).
- Merit Central/JPP captures information on merit increases, salary information, and employee performance ratings.

To assist FHFA in strengthening the protection of PII, we recommend the CTS and Merit Central/JPP system owners in coordination with the FHFA Chief Information Security Officer:

Recommendation 7: Determine the feasibility for automatically disabling inactive application accounts for CTS and Merit Central/JPP at a frequency that fits the business needs; and update applicable system policies and procedures, as necessary.

Recommendation 8: Implement a control at the application layer to ensure inactive application accounts for CTS and Merit Central/JPP are disabled in accordance with the determined system frequency. If the application does not accommodate automatic disabling of inactive accounts, then consider implementing manual compensating controls (i.e., manually reviewing and disabling dormant accounts) to help mitigate the risk.

5. FHFA Needs to Improve Its Management of Privacy Impact Assessments

One out of three information systems selected for testing, that house PII, did not accurately describe the PII collected in the PIA. Specifically, the PIA for the Merit Central/JPP System did not document the collection of social security numbers.

The FHFA SAOP stated that due to lack of sufficient oversight, the PIA was not consistently updated and reviewed to ensure accuracy of the PII collected for Merit Central/JPP, in accordance with the *FHFA Privacy Threshold Analysis and Privacy Impact Assessment Guide*.

NIST SP 800-53, Revision 4, Privacy Control AR-2, Privacy Impact and Risk Assessment, requires the organization to document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; and to conduct PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, states the following:

Audit of FHFA's 2019 Privacy Program

"A PIA must analyze and describe

- i. what information is to be collected (e.g., nature and source);
- ii. why the information is being collected (e.g., to determine eligibility);
- iii. intended use of the information (e.g., to verify existing data);
- iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- vi. how the information will be secured (e.g., administrative and technological controls); and..."

A PIA is both a tool and the outcome of a process which assists agencies in identifying and minimizing the privacy risks of policies, and/or systems. Agencies are required to conduct PIAs to ensure that programs or information systems comply with legal, regulatory, and policy requirements. If a PIA does not accurately reflect the information collected in the information system, it increases the risk that PII may be mishandled which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

To assist FHFA in strengthening the process for ensuring the accuracy of PIAs, we recommend the Senior Agency Official for Privacy, in coordination with the System Owner(s):

Recommendation 9: Review and update the Merit Central/JPP PIA to ensure it accurately describes all PII collected by the system.

Recommendation 10: Implement a process to ensure all of the agency's PIAs are consistently updated and reviewed to include all types of PII a system collects, in accordance with FHFA Privacy Threshold Analysis and Privacy Impact Assessment Guide.

6. FHFA Needs to Strengthen Its Privacy Training Program

FHFA's training records as of July 2018 showed only 80 percent of personnel, whose responsibilities include access to PII, completed required privacy role-based training on an annual basis.

The FHFA SAOP stated that privacy role-based training was only offered via an in-person session once a year and all users required to take the training did not attend due to scheduling conflicts. In addition, make-up training sessions were not offered due to the time constraints for delivering additional sessions. The SAOP stated that role-based privacy training will be conducted via a web based application in fiscal year 2019.

NIST SP 800-53, Revision 4, Privacy Control AR-5, Privacy Awareness and Training, requires the organization to administer targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII on an organizational-defined frequency, at least annually. FHFA's *Privacy Plan for Privacy Controls, April 2014*, requires that new employee and contractor personnel complete security related training before being granted access to FHFA's information systems. In addition, annual refresher training is provided to all employees and contractor

Audit of FHFA's 2019 Privacy Program

personnel with access to FHFA information systems. Role based privacy training is also provided to those employees and contractor personnel whose responsibilities include access to PII.

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.

To assist FHFA in strengthening the privacy training program, we recommend the FHFA Senior Agency Official for Privacy:

Recommendation 11: *Ensure all personnel whose responsibilities include access to PII complete annual privacy role-based training, whether via the planned web based application or by other means.*

EVALUATION OF MANAGEMENT COMMENTS

In response to a draft of this report, FHFA outlined its plans to address the recommendations. FHFA's comments are included in Appendix V.

FHFA management agreed with seven of the recommendations and disagreed with four of the 11 recommendations. Specifically, FHFA agreed with recommendations 1, 2, 3, 4, 9, 10 and 11 and disagreed with recommendations 5, 6, 7, and 8. We concur with management's responses to recommendations 1, 2, 3, 4, 9, 10, and 11. Our evaluation of management's response to recommendations 5, 6, 7, and 8 is below.

Recommendation Number	Evaluation of Management's Response
<p>Recommendation 5: Determine privacy controls that are information system-specific, and/or hybrid controls.</p> <p>Recommendation 6: Document privacy controls within each system's SSP or system-specific privacy plan, clearly identifying whether controls are program level, common, information system-specific, or hybrid.</p>	<p>While management disagreed with our recommendations, we note that in management's response that they are planning to address the recommendations with the release of NIST SP 800-53, Revision 5. Specifically, management stated they plan to perform a control mapping to the privacy controls documented in the subsequent release of NIST SP 800-53 and document any information system-specific-privacy controls within applicable SSPs. Specifically, FHFA stated,</p> <p style="padding-left: 40px;">“When officially released, FHFA will incorporate NIST 800-53 Revision 5, Appendix J Privacy Controls into the ISCM Strategy, and assess these controls annually, at the program level, as part of ISCM activities. Based on a review of the draft release of NIST 800-53 Revision 5, and the proposed creation of the Privacy Authorization (PA) control family, once NIST SP 800-53 Revision 5 is final, FHFA will perform a control mapping of the PA control family to determine which PA controls are information system-specific and which are organization specific. Information system-specific controls will be incorporated into the applicable information system security plans (SSPs) and will be assessed annually as part of FHFA's ISCM Strategy. FHFA will incorporate the NIST 800-53 Revision 5, Appendix J Privacy Controls within one year of the official NIST 800-53 Revision 5 publication date.”</p> <p>Accordingly, we consider management's response to meet the intent of our recommendations. As a result, no changes were made to the report.</p>

Audit of FHFA's 2019 Privacy Program

Recommendation Number	Evaluation of Management's Response
<p>Recommendation 7: Determine the feasibility for automatically disabling inactive application accounts for CTS and Merit Central/JPP at a frequency that fits the business needs; and update applicable system policies and procedures, as necessary.</p> <p>Recommendation 8: Implement a control at the application layer to ensure inactive application accounts for CTS and Merit Central/JPP are disabled in accordance with the determined system frequency. If the application does not accommodate automatic disabling of inactive accounts, then consider implementing manual compensating controls (i.e., manually reviewing and disabling dormant accounts) to help mitigate the risk.</p>	<p>Based on management's response, management has reached a decision to rely on disabling accounts at the network layer in lieu of disabling accounts at the application layer. However, this tailoring of controls has not been formally documented in accordance with NIST SP 800-53. NIST SP 800-53 states that tailoring of controls should be accompanied by risk-based determinations and incorporated into applicable SSPs. As such, we believe, consistent with Recommendation 7 and NIST guidance, that FHFA management formally documents a risk-based determination by documenting the current environment, risk analysis, and compensating controls; and update the applicable SSPs with the reference to the risk-based decision to fully support their control tailoring decision.</p>

Audit of FHFA's 2019 Privacy Program

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. 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 Senior Agency Official for Privacy/Chief Privacy Officer 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.

Audit of FHFA's 2019 Privacy Program

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.

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 Web sites 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 800-53, 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.

Audit of FHFA's 2019 Privacy Program

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 effective privacy and data protection policies and procedures.

Scope

CLA conducted this audit in accordance with performance auditing standards, as specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective.

The audit included tests of 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, Rev. 4, Appendix J, *Privacy Controls Catalog*.⁴ 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 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

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 information systems. We identified 11 systems within FHFA that housed privacy data and selected the following four systems listed below (**Table 2**).

⁴ Appendix J: Privacy Controls Catalog is available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

Audit of FHFA's 2019 Privacy Program

Table 2: Description of Systems Selected for Testing

Privacy System Name	Description
GSS ⁵	The FHFA GSS provides support for all information processing activities, internet access, and e-mail for FHFA.
CTS	CTS captures and tracks correspondence that FHFA receives from external sources. The system captures information on the sender and the nature of the correspondence (e.g., name; property, home, and business addresses; e-mail address; telephone numbers; and other personal and contact information, etc.). The system helps ensure FHFA responds to the inquiry in a timely and accurate manner.
Merit Central/JPP	Merit Central automates the calculation of the merit increases and annual bonuses based on various factors that include the employee's performance rating and current salary. Additionally, FHFA offices may distribute lump sum payments to employees in addition to merit increases. Office Directors use Merit Central to allocate lump sum payments to employees within their division. JPP allows FHFA employees and managers to complete their annual Job Performance Plan, Accomplishment Report, and Individual Development Plan, and allows rating officials to rate the employee's performance in accordance with FHFA's Performance Management Policy.
FOIAXpress	FOIAXpress, a commercial automated information system, tracks Freedom of Information Act (FOIA) requests. FOIA data consists of requests for information received from the public, and includes PII.

The audit also included an evaluation of whether FHFA took appropriate corrective action to address the findings and recommendations in the FHFA OIG Audit Report AUD-2017-007, *Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program*, issued August 30, 2017 (2017 Privacy Audit Report).

Audit fieldwork was performed at FHFA's headquarters in Washington, D.C., from March 27, 2019 to July 18, 2019.

Methodology

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

⁵ The FHFA GSS was included in testing because common access controls are used for some systems holding PII and users store data extracts on the GSS.

Audit of FHFA's 2019 Privacy Program

- 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 recommendations in the 2017 Privacy Audit Report, including supporting documentation to ascertain whether the actions taken addressed the weakness.⁶

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*, Appendix II, dated July 28, 2016
- 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*
- FHFA privacy-related policies and procedures

In selecting and testing for the adequacy and effectiveness of the privacy program, 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. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected, may be misleading.

⁶ Ibid. footnote 3.

Audit of FHFA's 2019 Privacy Program

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, Rev. 4, Appendix J, *Privacy Controls Catalog*.⁷ 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 OMB memoranda.

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 ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks.	AR-1 Governance and Privacy Program	Exceptions noted. See Finding #1
	Designate an SAOP who has agency-wide responsibility and accountability for 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, developing and evaluating privacy policy, and 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 structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any		Exceptions noted. See Finding #1

⁷ Appendix J: Privacy Controls Catalog is available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

Audit of FHFA's 2019 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control (s)	Results
	other information determined necessary by the agency's privacy program.		
	Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency.		Exceptions noted. See Finding #3.
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.
5	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, <i>Standards for Security Categorization of Federal Information and Information Systems</i> and NIST SP 800-60 Volume 1 Revision 1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i> .	SE-1 Inventory of Personally Identifiable Information	No exceptions noted.

Audit of FHFA's 2019 Privacy Program

#	Federal Criteria	NIST SP 800-53 Control (s)	Results
6	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.
7	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 #5.
8	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 5, 11 U.S.C. §552a (records maintained on individuals), internal controls, and other relevant matters.	AR-6 Privacy Reporting	No exceptions noted.
9	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	Exceptions noted. See Finding # 4.
10	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	Exceptions noted. See Finding # 6.
11	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 conducting privacy control assessments, and identifying metrics to determine whether privacy controls are implemented correctly,	AR-4 Privacy Auditing and Monitoring	Exceptions noted. See Finding #2.

Audit of FHFA's 2019 Privacy Program

#	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.		
12	<p>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.</p> <p>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.</p>	<p>AP-1 Authority to Collect</p> <p>DM-1 Minimization of Personally Identifiable Information</p>	No exceptions noted.
13	<p>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.</p>	AR-8 Accounting of Disclosures	No exceptions noted.
14	<p>Section 208 of the E-Government Act of 2002 Post privacy policies on agency Web sites used by the public.</p>	TR-3 Dissemination of Privacy Program Information	No exceptions noted.
15	<p>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.</p>	TR-2 System of Records Notices and Privacy Act Statements	No exceptions noted.
16	<p>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.</p> <p>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.</p>	CA-6 Security Authorization	Exceptions noted. See Finding #3.

Audit of FHFA's 2019 Privacy Program

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of our follow up related to the status of prior recommendations reported for the FY 2017 privacy audit.⁸

Finding #	Recommendations Prior Year 2017	Management Response	FHFA Actions Taken	Auditor's Position on Status
1	1. Conduct a comprehensive business process analysis to identify all FHFA business processes that collect PII in electronic and hardcopy form to build an inventory of where PII is stored.	FHFA agreed to identify those systems that collect and maintain PII, whether in electronic or paper format, to create an inventory by August 31, 2018.	FHFA's Privacy Office identified those systems that collect and maintain PII, both in paper and electronic format.	Closed
	2. Develop manual and automated processes to maintain an accurate and complete inventory of where PII is stored.	FHFA agreed to maintain an inventory of information systems that contain PII, in electronic and paper format, by August 31, 2018.	FHFA created a procedure to maintain the list of paper PII, in addition to the process that already existed to maintain an Information System Inventory that contains PII.	Closed
	3. Establish, implement, and train end users to apply naming conventions to files and folders containing PII.	FHFA agreed to work with appropriate stakeholders to review the feasibility of identifying and implementing naming conventions for FHFA files and folders that may contain PII by August 31, 2018. If FHFA determines that	FHFA and the Records and Information Management Group documented and finalized the Controlled Unclassified Information (CUI) policy and training has been developed related to naming conventions to files and folders containing PII. However, the procedures related to naming conventions to files and folders containing PII have	Open

⁸ Ibid. footnote 3.

Audit of FHFA's 2019 Privacy Program

Finding #	Recommendations Prior Year 2017	Management Response	FHFA Actions Taken	Auditor's Position on Status
		implementing naming conventions is feasible, FHFA will implement and train end users in such conventions by August 31, 2018.	not been finalized. Management stated that the procedures will be finalized by September 30, 2019.	
	4. Conduct a feasibility study of available technologies to supplement the manual and automated processes to identify and secure PII at rest and in transit.	FHFA agrees to review whether available technologies exist that may assist FHFA in identifying and security PII at rest and in transit by August 31, 2018.	On April 25, 2019, FHFA awarded a contract to purchase file analysis and PII discovery software.	Closed
2	1. Enhance System Owner training to include FHFA access control policies.	FHFA agrees to enhance system owner training to include FHFA access control policies.	FHFA enhanced their training program to include access controls.	Closed
	2. Review all privileged user accounts, obtain authorizations for users where none are currently documented, and remove access for those not authorized.	FHFA agrees and OTIM in collaboration with the system owners will review privileged user accounts to ensure that all active privileged user accounts have proper authorization, and remove access for those not authorized by March 30, 2018.	FHFA performed a privileged user account review to ensure all active privileged user accounts had proper authorization.	Closed

Audit of FHFA's 2019 Privacy Program

FHFA's MANAGEMENT RESPONSE



Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Deputy Inspector General for Audits

FROM: David A. Lee, Senior Agency Official for Privacy *David A. Lee*
R. Kevin Winkler, Chief Information Officer *Robert Kevin Winkler*

SUBJECT: Management Response to Draft Audit Report, *Performance Audit of the Federal Housing Finance Agency's (FHFA's) 2019 Privacy Program, dated July 18, 2019*

DATE: July 31, 2019

Thank you for the opportunity to respond to the above-referenced draft audit report by the Office of Inspector General (OIG). We are pleased that the audit concluded that FHFA had generally implemented effective privacy and data protection policies and procedures in accordance with law, regulation, and policy. This memorandum provides FHFA's management response to the recommendations contained in the OIG's draft audit report.

Maintenance of Privacy Policies and Procedures

Recommendation 1: *Develop and implement a process to ensure that FHFA's Privacy Program Plan, and privacy-related policies and procedures are reviewed and kept up-to-date at least on a biannual basis in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. The review and updates should be recorded, such as in a version history for each document.*

Management Response to Recommendation 1:

FHFA agrees with Recommendation 1. While FHFA privacy plans, policies and procedures were reviewed at least biennially and updated as necessary, FHFA did not formally document such reviews when no changes or updates were made to the privacy plans, policies and procedures. However, as of May 31, 2019, FHFA has updated and documented updates for the following plans, policies and procedures and included a version history indicating when the last time the plan, policy or procedure was reviewed:

1. Privacy Training Program Plan dated May 2019;
2. Program Plan for Privacy Controls dated May 2019;
3. Privacy Impact Assessment Guide dated May 2019;

Audit of FHFA's 2019 Privacy Program

Page 2 of 6

4. Guidelines on Disclosure of Information Contained in a Privacy Act System of Records dated May 2019;
5. Guidance on Amending or Correcting Records Contained in an FHFA System of Records dated May 2019;
6. Procedures for Monitoring FHFA's Website for Compliance with FHFA's Website Privacy and Social Media Policies dated February 2019;
7. Procedures for Monitoring IT Systems that Contain PII dated May 2019;
8. Procedures for SSN Collection dated May 2019;
9. Procedures for Updating and Maintaining and Inventory of Paper Holdings of PII July 2018;
10. Procedures on Drafting Privacy Act System of Records Notices dated May 2019; and
11. Protecting PII: Teleworking or Working Remotely dated May 2019.

FHFA has completed corrective actions to remediate this recommendation.

Privacy Continuous Monitoring

Recommendation 2: *Develop a schedule and/or rotation plan to assess privacy controls as required by FHFA's Privacy Continuous Monitoring Strategy.*

Recommendation 3: *Develop and implement a process to test privacy controls documented within the FHFA's Program Plan for Privacy Controls on at least an annual basis in accordance with the schedule and/or rotation to be developed as part of FHFA's Privacy Continuous Monitoring Strategy.*

Recommendation 4: *Develop and implement a process to identify and review metrics to measure the effectiveness of privacy activities and compliance with privacy requirements as specified by OMB.*

FHFA Response to Recommendations 2, 3, and 4:

FHFA agrees with Recommendations 2, 3, and 4. FHFA's Program Plan for Privacy Controls addresses privacy controls at the organization level. The FHFA SAOP is a participant in the security authorization process for all information systems that process PII, and ensures that privacy related risks have been addressed at the information system level, and that the security controls and enhancements implemented within the information system address applicable privacy risks. This is consistent with FHFA's Privacy Continuous Monitoring Strategy which refers to the ongoing assessment of controls (Information System Continuous Monitoring Strategy (ISCM)), which includes controls that also relate to Appendix J requirements (e.g., AR-4: User Re-Authorizations). Furthermore, FHFA has developed a Privacy Program Monitoring Program for 2019 where privacy controls in IT systems that contain PII will be reviewed and assessed. As of the date of this report, four out of nine systems have been reviewed with the remaining five scheduled to be completed by year-end 2019.

Audit of FHFA's 2019 Privacy Program

Page 3 of 6

Privacy Control Documentation

Recommendation 5: *Determine privacy controls that are information system-specific, and/or hybrid controls.*

Recommendation 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.*

FHFA Response to Recommendations 5 and 6:

FHFA disagrees with Recommendations 5 and 6. Per NIST 800-53 Revision 4, Privacy Controls are not specifically required at the information system level: "The privacy families can be implemented at the organization, department, agency, component, office, program, **or** information system level..." (emphasis added). Per NIST 800-37 Revision 2: "The senior agency official for privacy is responsible for designating which privacy controls may be treated as common controls. Privacy controls that are designated as common controls are documented in the organization's privacy program plan."

FHFA's Program Plan for Privacy Controls addresses privacy controls at the organization level. These controls are not specifically addressed within individual System Security Plans (SSP) as their implementation is common across FHFA, and are not uniquely implemented by individual information systems. This is consistent with FHFA's implementation of the Information Security Program Plan, which addresses organizationally common security controls owned and implemented by the information security team, rather than incorporating them into application-level SSPs when there is not an application-specific implementation of the control.

Furthermore, FHFA's SAOP is a participant in the security authorization process for all information systems that process PII, and ensures that privacy related artifacts (e.g., Privacy Threshold Assessments, Privacy Impact Assessments) have been completed, that privacy related risks have been addressed at the information system level, and that the security controls and enhancements implemented within the information system address applicable privacy risks. FHFA is following applicable federal guidance related to the implementation of privacy controls and therefore does not concur with this finding.

When officially released, FHFA will incorporate NIST 800-53 Revision 5, Appendix J Privacy Controls into the ISCM Strategy, and assess these controls annually, at the program level, as part of ISCM activities. Based on a review of the draft release of NIST 800-53 Revision 5, and the proposed creation of the Privacy Authorization (PA) control family, once NIST SP 800-53 Revision 5 is final, FHFA will perform a control mapping of the PA control family to determine which PA controls are information system specific and which are organization specific. Information system specific controls will be incorporated into the applicable information system security plans (SSPs) and will be assessed annually as part of FHFA's ISCM Strategy. FHFA

Audit of FHFA's 2019 Privacy Program

Page 4 of 6

will incorporate the NIST 800-53 Revision 5, Appendix J Privacy Controls within one year of the official NIST 800-53 Revision 5 publication date.

Protection of Information Systems from unauthorized access to PII

Recommendation 7: *Determine the feasibility for automatically disabling inactive application accounts for CTS and Merit Central/JPP at a frequency that fits the business needs; and update applicable system policies and procedures, as necessary.*

Recommendation 8: *Implement a control at the application layer to ensure inactive application accounts for CTS and Merit Central/JPP are disabled in accordance with the determined system frequency. If the application does not accommodate automatic disabling of inactive accounts, then consider implementing manual compensating controls (i.e., manually reviewing and disabling dormant accounts) to help mitigate the risk.*

FHFA Response to Recommendations 7 and 8:

FHFA disagrees with Recommendations 7 and 8. NIST 800-53 Revision 4, Access Control Enhancement 3 (AC-2 (3)), states that “The information system automatically disables inactive accounts after [Assignment: organization-defined time period].” FHFA disagrees that AC-2 (3) (inactivity lockout) applies to internal applications such as CTS, Merit Central, and JPP in addition to inactivity lockout on FHFA network accounts.

NIST 800-53 Revision 4 recommends that agencies conduct security control “tailoring” to identify common controls and perform “scoping” of remaining baseline security controls. FHFA performed security control tailoring following the release of NIST 800-53 Revision 4 and identified control AC-2 (3) as an “application specific” control for applications that utilize application specific login credentials (i.e., **do not** rely on FHFA’s Active Directory credentials for single sign-on) (emphasis added), as those applications must independently implement inactivity lockouts.

FHFA subsequently identified control AC-2 (3) as a “GSS Common Control” for applications that **do** rely on FHFA’s Active Directory credentials for access (via Windows Integrated Authentication) as those applications inherit the protection offered by Active Directory which disables dormant accounts that have been inactive after 35 days, preventing access to all FHFA systems.

CTS, Merit Central, and JPP rely on FHFA’s Active Directory credentials which support single sign-on capability. An additional application inactivity lockout, based on when each system was last accessed, is not specifically required by NIST nor would it be effective given that if FHFA’s network is not accessed for 35 days, access to the network and any associated systems are automatically disabled. Furthermore, FHFA system owners are provided regular IT Security and Privacy Awareness training on the importance of monitoring system users and activity.

Audit of FHFA's 2019 Privacy Program

Page 5 of 6

Annually, FHFA system owners must re-certify system users and their access levels. In addition, system owners or their designees receive audit logs which contain system access to determine if any accounts can be removed as well as to review for unusual or suspicious activity. As such FHFA is in compliance with AC-2(3) and, therefore, FHFA does not believe that conducting a feasibility study (recommendation 7) or implementing additional controls at the application level (recommendation 8) are either required or warranted.

Privacy Impact Assessments

Recommendation 9: *Review and update the Merit Central/JPP Privacy Impact Assessment (PIA) to ensure it accurately describes all PII collected by the system.*

Recommendation 10: *Implement a process to ensure all of the Agency's PIAs are consistently updated and reviewed to include all types of PII a system collects, in accordance with FHFA Privacy Threshold Analysis and Privacy Impact Assessment Guide.*

FHFA response to Recommendations 9 and 10:

FHFA agrees with Recommendations 9 and 10.

FHFA issued a revised [JPP/Merit Central PIA](#) on May 23, 2019. Therefore, FHFA has completed the corrective action to remediate Recommendation 9.

FHFA has a process, as set forth in FHFA's *Privacy Impact Assessment Guide, Revision 2*, dated May 2019, where PIAs are reviewed and updated as needed, depending upon the nature and the extent of changes made to systems covered by an existing PIA. Therefore, FHFA has completed a corrective action to remediate Recommendation 10.

Privacy Training Program

Recommendation 11: *Ensure all personnel whose responsibilities include access to PII complete annual privacy role-based training, whether via the planned web based application or by other means.*

FHFA response to Recommendation 11:

FHFA agrees with Recommendation 11. FHFA employees, who by virtue of their position or access to or use of PII, are required to complete Mandatory Annual Role-Based Privacy Training. This training was conducted in fiscal years 2018 and 2019, as well as prior years. For fiscal year 2019, in order to ensure that employees were completing the training, FHFA utilized its Learning Management System (LMS) to provide this training. LMS records when the training has been completed, thus allowing the Privacy Office to better track who has and has not completed the training. As of July 26, 2019, 99.5% of those required to take this training have completed it. For personnel who do not complete the training, FHFA may suspend their network

access, until they complete the training. Therefore, FHFA has completed the corrective action to remediate this recommendation.

If you have any questions, please contact Stuart Levy.

CC: C. Bosland
L. Stauffer
T. Leach
C. Sherman
J. Major
R. Mosios

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