Federal Housing Finance Agency
Office of Inspector General

Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program

On September 26, 2017, Kearney & Company revised its report on FHFA's Privacy Program to reflect the rescission of Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)*, and the requirement to log data extracts of PII. This revised report removes Recommendation 5 from Finding 1. FHFA's management response was not updated to reflect this change.

Audit Report • AUD-2017-007 • August 30, 2017

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

August 30, 2017

TO: Melvin L. Watt, Director

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

SUBJECT: Audit Report - *Performance Audit of the Federal Housing Finance Agency's (FHFA) 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 Kearney & Company, P.C. (Kearney) 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, Kearney concluded that FHFA effectively implemented six of the nine privacy requirements in 42 U.S.C. §2000ee-2, in addition to applicable privacy controls listed under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, Appendix J, *Privacy Controls Catalog*. In its report, Kearney made seven recommendations to ensure FHFA identifies, monitors, and protects the personally identifiable information (PII) it collects and to ensure that privileged user access is approved and documented. In its management response, FHFA agreed to implement the recommended corrective actions.

In connection with the contract, we reviewed Kearney'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 listed in NIST SP 800-53. Kearney is responsible for the attached auditor's report dated August 30, 2017, and the conclusions expressed therein. However, our review found no instances where Kearney did not comply, in all material respects, with generally accepted government auditing standards.

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 Banking, Housing, and Urban Affairs
- 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 Financial Services
- Committee on Oversight and Government Reform

Performance Audit of the Federal Housing Finance Agency's (FHFA) Privacy Program

August 30, 2017

This report was revised and Recommendation 5 for Finding 1 was removed on September 26, 2017 to reflect the rescission of OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)*, and the requirement to log data extracts of PII. FHFA's management response was not updated to reflect this change.

Point of Contact:
Tyler Harding, Principal
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
Tyler.Harding@kearneyco.com
Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

TABLE OF CONTENTS

Page

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

COVER LETTER

August 30, 2017

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

Dear Inspector General Wertheimer:

Kearney & Company, P.C. (defined as "Kearney," "we," and "our" in this report) is pleased to provide this Privacy Program Audit Report, which details the results of our audit of the Federal Housing Finance Agency's (FHFA or Agency) implementation of specific security and privacy controls as directed in Section 522 of the Consolidated Appropriations Act of 2005, Division H, and updated in 42 United States Code (U.S.C.) § 2000ee-2. The FHFA Office of Inspector General (OIG) contracted with Kearney to conduct this independent assessment as a performance audit under Generally Accepted Government Auditing Standards (GAGAS).

The objective of this audit was to report on the effectiveness of FHFA's information security and privacy practices, with a focus on FHFA's implementation of privacy controls and the following nine requirements identified in 42 U.S.C. § 2000ee-2:[1]

- Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form
- 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
- 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
- Evaluating legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the Federal Government
- Conducting a privacy impact assessment (PIA) of proposed rules of the Agency on the privacy of information in an identifiable form, including the type of Personally Identifiable Information (PII) collected and the number of people affected

[1] The full text of 42 U.S.C. is available at: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title42-section2000ee-2&num=0&edition=prelim.

- Preparing a report (i.e., annual Federal Information Security Modernization Act of 2014 [FISMA] Privacy Report) and submitting it to Congress on an annual basis on activities of the Agency that affect privacy, including complaints of privacy violations, implementation of 5 U.S.C. § 552a, internal controls, and other relevant matters
- Ensuring that the Agency protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction
- Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies
- Ensuring compliance with the Agency's established privacy and data protection policies.

Kearney's methodology for the fiscal year (FY) 2017 Privacy Program audit included an assessment of seven[2] FHFA information systems for compliance with selected controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, found in Appendix J, *Privacy Control Catalog*.

We conducted this performance audit in accordance with GAGAS. 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.

Based on our audit work, Kearney concluded that FHFA has effectively implemented seven of the nine privacy requirements in 42 U.S.C. § 2000ee-2, in addition to applicable privacy controls listed under NIST SP 800-53, Rev. 4, Appendix J, *Privacy Controls Catalog*.[3] In this report, we made six recommendations for improvements to ensure FHFA adequately identifies, monitors, and protects the complete inventory of its PII holdings and appropriately approves and documents privileged user access.

[2] Kearney sampled the following FHFA systems: General Support System (GSS), Job Performance Plan (JPP), Correspondence Tracking Systems (CTS), Content Management Interface (CMI), Micro iComplaints, FedHR (FHR) Navigator, and Everbridge. Of the seven sampled systems, all systems stored and processed PII, except CMI.

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

In closing, we appreciate the courtesies extended to the Kearney Audit Team by FHFA during this engagement.

Sincerely,

Kearney & Company, P.C.
Alexandria, VA

OVERVIEW

Purpose

Kearney was contracted by OIG to perform an audit of the Agency's Privacy Program. This report satisfies a requirement in 42 U.S.C. § 2000ee-2 that Inspectors General (IG) periodically review their respective agencies' Privacy Programs.

Background

On July 30, 2008, FHFA was established by the Housing and Economic Recovery Act of 2008 (HERA), Public Law (P.L.) No. 110-289. HERA abolished two existing Federal agencies (i.e., the Office of Federal Housing Enterprise Oversight and the Federal Housing Finance Board) and created FHFA to regulate the Federal National Mortgage Association (Fannie Mae); the Federal Home Loan Mortgage Corporation (Freddie Mac); the Federal Home Loan Bank System, composed of 11 Federal Home Loan Banks (FHLBanks); and the FHLBanks' fiscal agent, the Office of Finance.

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 FHLBanks, and the Office of Finance. The Agency also currently serves as conservator for Fannie Mae and Freddie Mac. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the 11 FHLBanks.

Federal Privacy Program Requirements

Section 522 of Consolidated Appropriations Act of 2005, Division H,[4] as originally enacted, required the IG of each agency to perform an evaluation every two years to assess its agency's use of information in identifiable form, evaluate the privacy and data protection procedures of the agency, and recommend strategies and specific steps to improve privacy and data protection management. Section 742(b) of the Consolidated Appropriations Act of 2008, Division D[5] amended this review requirement by mandating that IGs conduct these reviews periodically (instead of biennially), as well as report the results of the reviews to the House of Representatives and Senate Committees on Appropriations, the House of Representatives Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs.

The Privacy Act of 1974 (5 U.S.C. § 552a), as amended, requires agencies to collect only an individual's information that is relevant and necessary to accomplish a purpose of the agency required 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

[4] P.L. 108-447, which became law on December 8, 2004.
[5] P.L. 110-161, which became law on December 26, 2007.

result in substantial harm, embarrassment, inconvenience, or unfairness to any individual for whom the information is maintained, and must not disclose this information except under certain circumstances (e.g., need to know within the agency, required Freedom of Information Act [FOIA] disclosure, or statistical research).

In addition, Section 208 of the E-Government Act of 2002 (P.L. 107-347) requires agencies to: 1) conduct PIAs of information technology (IT) 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.

Prior Privacy Audit Results from September 2014

OIG contracted with an independent audit firm to conduct a Privacy Program audit based on 42 U.S.C. § 2000ee-2 for FHFA's Privacy Program in September 2014.[6] In 2014, the firm made six recommendations for FHFA to strengthen its 2014 Privacy Program. Subsequently, OIG determined that FHFA took corrective actions to address all recommendations and closed the six recommendations. Appendix C: Status of Prior-Year Findings lists each recommendation and describes the corrective actions taken by FHFA.

AUDIT CRITERIA

Kearney's performance audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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:

- E-Government Act of 2002
- OMB Circular A-130, *Managing Information as a Strategic Resource,* Appendix II, dated July 28, 2016
- OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*
- OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*.

[6] OIG, *CliftonLarsenAllen, LLP's Independent Audit of the Federal Housing Finance Agency's Privacy Program–2014* (AUD-2014-020), dated September 26, 2014.

NIST Security Standards and Guidelines

NIST provides standards and guidelines pertaining to Federal information systems. The standards prescribe information security requirements necessary to improve the security, privacy, and overall protection of Federal information and information systems. Federal agencies must comply with NIST's Federal Information Processing Standards (FIPS) Publications (PUB) and SPs as recommended guidance documents. The following NIST FIPS PUBs and SPs were referenced during the FHFA Performance Audit of the Privacy Program:

- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems; A Security Life Cycle Approach*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Appendix J, *Privacy Control Catalog*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*.

RESULTS OF AUDIT

Kearney executed testing of the FHFA Privacy Program based upon 42 U.S.C. § 2000ee-2 (requirements and IT application security controls), the Privacy Act of 1974, E-Government Act of 2002, Section 208 of the E-Government Act of 2002, OMB memoranda, and applicable NIST guidance on privacy. A summary of test results for these controls is identified in APPENDIX B: TEST MATRIX. The following sections identify improvements since the 2014 audit of the Privacy Program, resolution of issues identified in that audit, and findings with recommendations for improvement regarding the Privacy Program's inventory and system access.

Privacy Program Improvements Since the September 2014 Privacy Program Report

Kearney noted that FHFA updated its privacy policies to address changes in applicable laws and OMB guidance since the prior 2014 OIG Privacy Program audit. FHFA's privacy policies are posted on the intranet and FHFA's public website, which is periodically updated to reflect revisions to policies and procedures. In addition, the FHFA Senior Agency Official for Privacy (SAOP) stated that FHFA is migrating all hardcopy PII to electronic records or digital images.

Resolution of Prior-Year Issues

In 2014, OIG engaged an independent audit firm to audit FHFA's Privacy Program; the auditor identified two control deficiencies and made six recommendations for improvement. Following the 2014 Report, OIG reviewed and accepted FHFA's completed corrective actions to implement and track the logging and control of all computer-readable data extracts of PII, conduct periodic reviews of website compliance with privacy requirements, and track and timely complete

corrective actions identified in website compliance reviews. Please see Appendix C: Status of Prior-Year Findings for more information.

FINDING 1

Lack of a Complete and Accurate Personally Identifiable Information Systems Inventory

Developing and maintaining a complete and accurate inventory of where PII is collected and stored is an essential step in securing and protecting PII from accidental disclosure. Both the Privacy Act of 1974 and FISMA require all Federal agencies to protect and secure PII from disclosure.

In the execution of its mission, FHFA collects PII in both hardcopy and electronic forms. Kearney noted that FHFA's Privacy Program does not maintain a complete and accurate inventory of PII stored in hardcopy and electronic forms. While FHFA has an inventory of information systems storing PII, this inventory does not include PII stored in unstructured data stores, such as SharePoint or network shared drives (e.g., FHFA's :\M drive). Further, the PII inventory does not include hardcopy data stores, such as background investigation or Human Resources (HR) records.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, *Privacy Control Catalog*, established several Federal privacy protection mandates:

> "*SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION*
>
> The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from PIA for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII.
>
> *AR-4 PRIVACY MONITORING AND AUDITING*
>
> Control: The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation. Supplemental Guidance: … Organizations also: (i) implement technology to audit for the security, *appropriate* use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy

requirements; and (iv) ensure that corrective actions *identified* as part of the assessment process are tracked and monitored until audit findings are corrected. The organization SAOP/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials."

FHFA had once developed a listing of physical PII holdings, but it has not updated or maintained the inventory of PII, as the Agency has prioritized digitizing all hardcopy PII records and storing the records within defined information systems. Since then, FHFA has not conducted a comprehensive business process analysis to identify all business functions that collect, process, and store PII. While FHFA has identified significant business applications that collect, process, and store PII, the Agency has not compiled a complete and accurate inventory of where PII records exist in unstructured or hardcopy form. Further, FHFA presently lacks manual and automated processes to discover and maintain a complete inventory of where PII is stored in unstructured and hardcopy form. Manual processes include, but are not limited to, activities such as periodic, manual searches of SharePoint sites and network shared drives, routine physical walkthroughs of FHFA offices, and training end users to apply appropriate naming conventions for files and folders containing PII.

Without a complete inventory of where PII resides, FHFA is unable to adequately monitor its collections of PII for compliance with privacy laws, regulations, and guidelines. This includes ensuring proper access restrictions are in place to only allow access to those who need the PII data to perform their official duties and confirming that the organization only captures, stores, and maintains PII where absolutely necessary.

Recommendations: Kearney recommends that the FHFA Privacy Office:

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.
2. Develop manual and automated processes to maintain an accurate and complete inventory of where PII is stored.
3. Establish, implement, and train end users to apply naming conventions to files and folders containing PII.
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.

FINDING 2

Lack of Account Requests and Approvals for Privileged Users

Organizations implement access controls and associated procedures to ensure adequate consideration and appropriate approval when granting elevated privileges to users within IT and information system boundaries. Specifically, an effective access control process protects systems and applications from unauthorized access and enforces the principle of least privilege. Proper authorization and documentation of users requesting or granted privileged access is essential for traceability and for maintaining a secure IT environment. NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, establishes that users requiring administrative privileges for their respective information system accounts undergo additional review by appropriate personnel, given their elevated privileges.

FHFA's policies for each of the seven sampled systems[7] state that to obtain elevated privileges, a user must first obtain approval, in writing, from the respective System Owner. In regards to the FHFA GSS, access is requested through the Access Control System (ACS).

To verify whether FHFA System Owners properly followed documented access control procedures in regards to creating and approving privileged access, Kearney sampled nine administrators from a population of 37 across the seven sampled systems. Subsequently, we requested the access approval documentation for each sampled user for inspection and testing purposes.

Kearney noted that FHFA did not consistently follow its account provisioning policies outlined in its *Access Control Standard* and did not retain evidence of System Owner approval for seven of nine privileged user accounts.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, established the following mandates relating to access control:

> "*AC-2 Account Management*
>
> Control: An organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account and requires approvals by appropriate personnel (System Owners) for access to be granted to information systems.

[7] Kearney sampled the following FHFA systems: GSS, JPP, CTS, CMI, Micro iComplaints, FHR Navigator, and Everbridge. Of the seven sampled systems, all systems stored and processed PII, except CMI.

AC-6 Least Privilege

Control: An organization explicitly authorizes access to systems and applications, including administrative access. That access should be documented, including rationale for such access."

In addition to NIST SP 800-53, Rev. 4, FHFA's *Access Control Standard*, dated June 2016, states:

"FHFA information owners and system owners shall ensure that only users with a valid need (i.e., in the performance of their official duties or duties under an authorized contract) are provided access to Non-Public or Non-Public Restricted information, and that they are provided with the lowest level of access to the data (i.e., read only) necessary to perform their job function.

Privileged access authorizations must be approved by the system owner and include a written justification in the form of a help desk or access control ticket."

Kearney noted that System Owners did not follow privileged user access control procedures because user accounts were created as systems were placed into production. Additionally, System Owners were not aware of FHFA's *Access Control Standard*.

Without evidence of written approval, FHFA cannot demonstrate that the individuals obtained privileged access through authorized means.

Recommendations: Kearney recommends that FHFA:

1. Enhance System Owner training to include FHFA access control policies.
2. Review all privileged user accounts, obtain authorizations for users where none are currently documented, and remove access for those not authorized.

CONCLUSION

Based on our audit work, we concluded that FHFA has effectively implemented seven of the nine privacy requirements in 42 U.S.C. § 2000ee-2. In its management response, provided in Appendix D, FHFA agreed to implement the recommended corrective actions.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

Kearney executed testing of the FHFA Privacy Program based upon 42 U.S.C. § 2000ee-2, the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, OMB memoranda, and applicable NIST privacy guidance.

Scope

The objective of this performance audit was to report on the effectiveness of FHFA information security and privacy practices, with a focus on FHFA's implementation of privacy controls. This report is presented to OIG to address its requirements under 42 U.S.C. § 2000ee-2. We identified and assessed the implementation of selected privacy controls for a representative sample of FHFA systems containing PII. Kearney identified 15 systems within FHFA with privacy data and selected the following six systems listed in ***Table 1*** in addition to the FHFA GSS.[8]

Table 1: FHFA PII Systems Assessed

Privacy System Name	Description
FHFA Network Infrastructure (GSS)	The FHFA GSS provides support for all information processing activities, internet access, and e-mail for FHFA.
CTS	The purpose of this system is to capture and track 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). The system helps ensure FHFA responds to the inquiry in a timely and accurate manner.
Everbridge	Everbridge is a web-based system that allows FHFA's Office of Facilities Operation Management (OFOM) personnel or other authorized employees to send notifications to FHFA employees using lists, locations, and visual intelligence. The Everbridge mass notification system keeps Agency employees informed before, during, and after events.
FHR Navigator	The purpose of this system is to automate Federal HR functions within a single platform. It is a suite of web-based software tools that is bolstered by a centralized database to support the strategic management of human capital within the Federal workplace.
Micro iComplaints	This system is used to track, manage, and report on Equal Employment Opportunity (EEO) complaints. Information collected is kept confidential for use during the alternate dispute resolution process. Additionally, data is used to create statistical reports.

[8] 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.

Privacy System Name	Description
Merit Central/JPP	This system is an automated tool that facilitates annual FHFA-wide merit increase and Performance-Based Bonus (PBB) decision-making and processing, as well as conducts salary planning determinations. The Office of Human Resources Management (OHRM) and OTIM JPP worked in close coordination to develop this internal system.
CMI (Content Management System)[9]	CMI is a moderate-impact system that allows individuals to publish content on the FHFA.gov website.

Kearney performed fieldwork for the FHFA Privacy Program audit from April to July 2017. Throughout the Privacy Program audit, we met with FHFA management to discuss preliminary observations. In addition to the Federal audit criteria listed above (see Appendix C: Status of Prior-Year Findings), Kearney's work in support of the audit was guided by applicable FHFA policies, including the following:

- *General Support Systems (GSS) Information Security Architecture*
- *Security Awareness and Training Procedures*
- *Information Security Incident Response Plan*
- *Procedures for Monitoring of Information Technology Systems that Contain Personally Identifiable Information*
- *Security Assessment and Authorization Procedure*
- *Identification and Authentication Standard*
- *Access Control Standard*
- *Privacy Program Plan*
- *Use and Protection of Personally Identifiable Information Policy*.

As a part of the privacy audit, Kearney evaluated access to information systems containing PII. We observed that privileged users for the sampled systems had the greatest access to PII and presented the most risk. Therefore, Kearney sampled nine of 37 privileged users across the selected systems to confirm that the selected privileged users were authorized by their respective System Owners or other appropriate officials.

[9] While CMI was included in our sampled systems, Kearney determined that the system does not store or process PII.

APPENDIX B: TEST MATRIX

The purpose of the matrix below is to identify the nine requirements identified in Section 522 of Consolidated Appropriations Act of 2005, Division H and 42 U.S.C. § 2000ee-2 for FHFA's Privacy Program, in addition to applicable privacy controls listed under NIST SP 800-53, Rev. 4, Appendix J, *Privacy Controls Catalog*.[10] 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 other OMB memoranda.

Kearney tested the following entity and system-level control objectives to conclude on FHFA's Privacy Program. We noted two findings with regards to the Privacy Program's lack of a complete inventory and lack of written management authorizations for privileged users. See ***Table 2*** and ***Table 3*** for Kearney's conclusions on tests performed during the audit.

Table 2: Privacy Program Reporting Audit 42 U.S.C. § 2000ee-2 Requirements

#	42 U.S.C. § 2000ee-2 Requirements	NIST SP 800-53 Control (s)	Kearney Test Results
1	Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form	AR-7	Demonstrates Effectiveness
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	AR-4	Demonstrates Effectiveness
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. [*Emphasis placed on maintaining an inventory of PII holdings*.]	AR-6, SE-1	Warrants Management Attention (See **Finding** 1)
4	Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government	AR-6	Demonstrates Effectiveness
5	Conducting 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	Demonstrates Effectiveness

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

#	42 U.S.C. § 2000ee-2 Requirements	NIST SP 800-53 Control (s)	Kearney Test Results
6	Preparing a report (i.e., annual FISMA Privacy Report) to Congress on an annual basis on activities of the Agency that affect privacy, including complaints of privacy violations, implementation of 5 U.S.C. § 552a, internal controls, and other relevant matters	AR-6	Demonstrates Effectiveness
7	Ensuring that the Agency protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction	AR-2, AR-6, AR-8, DI-2	Warrants Management Attention (See **Finding** 2)
8	Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies	AR-3, AR-5	Demonstrates Effectiveness
9	Ensuring compliance with the Agency's established privacy and data protection policies	AR-1	Demonstrates Effectiveness

From NIST SP 800-53, Rev. 4, Appendix J, *Privacy Controls Catalog*, Kearney selected privacy controls relevant to FHFA's Privacy Program. ***Table 3*** presents Kearney's test results for the sampled privacy controls.

Table 3: Additional NIST SP 800-53, Rev. 4, Appendix J, Privacy Controls

#	Additional NIST Privacy Controls	NIST SP 800-53 Control (s)	Kearney Test Results
10	The Agency has determined and documented the legal authority that permits the collection, use, or maintenance of PII for a specific program or information system used.	AP-1, TR-2	Demonstrates Effectiveness
11	The organization describes the purpose for which PII is collected, used, maintained, and shared in its privacy notices.	AP-2	Demonstrates Effectiveness
12	The Agency takes reasonable steps to ensure the accuracy and relevance of PII being used by information systems or programs.	DI-1	Demonstrates Effectiveness
13	The Agency takes appropriate steps to identify the minimum PII elements relevant and necessary to accomplish the purpose of collection for information system(s).	DM-1	Demonstrates Effectiveness
14	The Agency disposes of and/or anonymizes PII in accordance with a National Archives and Records	DM-2	Demonstrates Effectiveness

#	Additional NIST Privacy Controls	NIST SP 800-53 Control (s)	Kearney Test Results
	Retention (NARA)-approved record retention schedule and reduces misuse or unauthorized access of PII.		
15	The Agency develops and implements a Privacy Incident Response Plan addressing incidents involving PII.	SE-2	Demonstrates Effectiveness
16	The Agency provides notice to the public of the privacy information practices and the impact of their programs and activities.	TR-1, TR-3, IP-2, IP-3	Demonstrates Effectiveness

APPENDIX C: STATUS OF PRIOR-YEAR FINDINGS

Kearney obtained the audit results from the prior Privacy Program audit (September 2014) to gain a better understanding of FHFA's Privacy Program and corrective actions taken to address previous risks. The table below presents the status of prior Privacy Program findings. In regards to the prior audit findings from 2014, all six of the recommendations were closed by OIG based on the corrective actions taken by FHFA.

#	Recommendations PY 2014	Management Response	FHFA Actions Taken	Status
1	Document, disseminate, and implement a policy requiring the logging and control of all computer-readable data extracts from databases holding PII.	"FHFA agrees with these recommendations and will draft and issue a policy requiring the logging and control of all computer readable data extracts from databases holding PII. In addition, FHFA will draft procedures on erasing such data extracts after 90 days or require a justification for continued retention beyond 90 days. Furthermore, procedures will be drafted on how to track those extracts that are retained beyond 90 days. FHFA will complete this by no later than September 18, 2015."	FHFA updated existing procedures regarding monitoring of IT systems that contain PII to address this finding. Specifically, new procedures were added that require System Owners to verify, at least annually, that computer-readable data extracts containing PII are deleted within 90 days of their extraction or that adequate justification from the user was received for the continued need for the data extract. These procedures were posted to FHFA's intranet and incorporated into OTIM's IT System Re-Authorization form.	Closed –OIG accepted corrective actions completed by FHFA as responsive to address this finding.
2	Verify that each extract containing PII is erased within 90 days or adequate justification is provided for retention.			Closed –OIG determined that management's proposed actions were responsive to the audit.
3	Tracks extracts containing PII and retained beyond 90 days to ensure they are erased when no longer required.			Closed –OIG determined that management's proposed actions were responsive to the audit.
4	Document, disseminate, and implement a policy requiring periodic, but at least annual, reviews of	"We have reviewed FHFA's 'Procedures for Monitoring FHFA's Website for Compliance with FHFA's	FHFA's website privacy and social media policies were developed and circulated to the affected stakeholders. FHFA	Closed –OIG accepted corrective actions completed by FHFA as responsive to address this finding.

#	Recommendations PY 2014	Management Response	FHFA Actions Taken	Status
	website compliance with privacy requirements.	Website Privacy and Social Media Policies' and a corresponding Agency memo detailing the results of a scan on FHFA's websites, which supports the Agency's corrective actions for recommendation 4 in the subject report. FHFA had responded that it would draft and issue a policy requiring at least annual reviews of agency websites to ensure compliance with FHFA's privacy requirements."	planned monitoring and completion in a timely manner.	
5	Conduct periodic reviews of FHFA-owned publicly accessible websites to ensure compliance with Agency policy.	"We obtained the periodic website compliance reviews that FHFA's webmaster conducted, along with evidence the sole matter identified during the reviews was corrected. We conclude that the Agency's actions are responsive to the agreed-upon corrective actions and consider this recommendation closed." FHFA agreed to issue a policy requiring at least annual reviews of agency websites to	FHFA completed a review of its website to determine compliance with the Agency's website privacy and social media policies in March 2015.	Closed –OIG accepted corrective actions completed by FHFA as responsive to address this finding.
6	Track all corrective actions identified in website compliance reviews and ensure the actions are completed in a timely manner.		The Privacy Office provided evidence of tracking the one item listed in the March 2015 review and planned to follow up with the Webmaster to ensure that this corrective action is completed before the next review.	Closed –OIG accepted corrective actions completed by FHFA as responsive to address this finding.

#	Recommendations PY 2014	Management Response	FHFA Actions Taken	Status
		ensure compliance with FHFA's privacy requirements.		

APPENDIX D: FHFA'S MANAGEMENT RESPONSE

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Deputy Inspector General for Audits

FROM: David A. Lee, Managing Associate General Counsel and Senior Agency Official for Privacy
R. Kevin Winkler, Chief Information Officer

SUBJECT: Federal Housing Finance Agency's (FHFA) Response to FHFA Office of Inspector General Draft Audit Report, *Performance Audit of the Federal Housing Finance Agency's Privacy Program*, dated August 17, 2017

DATE: August 28, 2017

This memorandum provides FHFA's management response to the recommendations contained in the draft audit report titled *Performance Audit of the Federal Housing Finance Agency's Privacy Program*.

Recommendation 1: OIG recommends that the FHFA Privacy Office:

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.
2. Develop manual and automated processes to maintain an accurate and complete inventory of where PII is stored.
3. Establish, implement, and train end users to apply naming conventions to files and folders containing PII.
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.
5. Design and implement automated and manual processes to satisfy the OMB Memorandum M-07-16 requirement to log all data extracts of PII and confirm that PII has been deleted after 90 days or when no longer needed.

FHFA Response:

1. FHFA agrees to identify those systems that collect and maintain PII, whether in

electronic or paper format, to create an inventory by August 31, 2018.

2. FHFA agrees to maintain an inventory of systems that contain PII, in both electronic and paper format, by August 31, 2018.
3. FHFA agrees 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 implementing naming conventions is feasible, FHFA will implement and train end users in such conventions by August 31, 2018.
4. FHFA agrees to review whether available technologies exist that may assist FHFA in identifying and securing PII at rest and in transit by August 31, 2018.
5. FHFA agrees to review its current manual process and determine whether any changes need to be made. In addition, FHFA agrees to review whether any automated processes exist, and implement as appropriate, to satisfy OMB M-07-16 requirement to log data extracts of PII and confirm that the PII from those data extracts is deleted after 90 days or when no longer needed by August 31, 2018.

Recommendation 2: OIG recommends that FHFA:

1. Enhance System Owner training to include FHFA access control policies.
2. Review privileged user accounts, obtain authorizations for users that do not have proper authorization, and remove access for those not authorized.

FHFA Response:

1. FHFA agrees to enhance system owner training to place additional emphasis on FHFA access control policies and procedures by March 30, 2018.
2. 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.

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

CC: T. Leach
J. Major
R. Mosios
C. Sherman

APPENDIX E: ACRONYM LISTING

Acronym	Definition
ACS	Access Control System
CMI	Content Management Interface
CPO	Chief Privacy Officer
CTS	Correspondence Tracking System
DLP	Data Loss Prevention
Fannie Mae	Federal National Mortgage Association
FHFA	Federal Housing Finance Agency
FHFB	Federal Housing Finance Board
FHLBanks	Federal Home Loan Banks
FHR	Federal Human Resources
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
Freddie Mac	Federal Home Loan Mortgage Corporation
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
HERA	Housing and Economic Recovery Act of 2008
HR	Human Resources
iComplaints	Micro iComplaints
ID	Identification
IT	Information Technology
JPP	Job Performance Plan
Kearney	Kearney & Company, P.C.
NIST	National Institute of Standards and Technology
OFHEO	Office of Federal Housing Enterprise Oversight
OIG	Office of Inspector General
OHRM	Office of Human Resources Management
OMB	Office of Management and Budget
OTIM	Office of Technology and Information Management
P.L.	Public Law
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PUB	Publication
Rev.	Revision
SAOP	Senior Agency Official for Privacy
SP	Special Publication
U.S.	United States
U.S.C.	United States Code

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

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

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

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

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