FEDERAL HOUSING FINANCE AGENCY
OFFICE OF INSPECTOR GENERAL

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Privacy Program and Implementation - 2011

Audit Report: AUD-2011-003 **Dated: September 30, 2011**

FEDERAL HOUSING FINANCE AGENCY
OFFICE OF INSPECTOR GENERAL
AT A GLANCE

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Privacy Program and Implementation - 2011

Why FHFA-OIG Contracted for Audit

Section 522 of the Consolidated Appropriations Act of 2005 (Section 522), as amended, requires that each agency designate a Chief Privacy Officer 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 relating to agency employees and the public. Additionally, Section 522 requires the Inspector General of each agency to periodically review the agency's implementation of the requirements of Section 522 including the agency's privacy program.

A comprehensive privacy program helps to ensure that risks related to the collection, storage, transmission, and destruction of personally identifiable information (PII)—such as an individual's name, date of birth, and social security number—are mitigated. A strong privacy program also provides a framework for the agency to consider the implications of business decisions made as they pertain to PII. A privacy program should also help maintain public trust and confidence in an organization, protect the reputation of an organization, and protect against legal liability for an organization by providing the necessary safeguards to minimize the risk of unintended disclosure of PII.

The Federal Housing Finance Agency (FHFA or Agency) Office of Inspector General (FHFA-OIG) contracted with Clifton Gunderson LLP (CG) to conduct a performance audit to fulfill its Section 522 responsibilities for a periodic review of FHFA's privacy program and its implementation. The objective of this performance audit was to assess FHFA's privacy program and its implementation, including compliance with the statutory and regulatory requirements concerning the protection of PII. The specific sub-objectives were to determine whether FHFA implemented comprehensive privacy and data protection procedures as required by Section 522 and accurately reported on its use of information in an identifiable form (also referred to as PII), along with its privacy and data protection policies and procedures.

What FHFA-OIG Recommends

FHFA-OIG adopted CG's findings and nine recommendations to FHFA to assist in strengthening its privacy program.

In response to FHFA-OIG's findings and recommendations, FHFA provided written comments, dated September 26, 2011. The Agency agreed with the recommendations. The complete text of the written comments can be found in Appendix B of this report.

What Clifton Gunderson LLP Found (See Appendix A of this Report)

While FHFA's privacy program had a number of strengths, such as a policy on the use and protection of PII, FHFA did not meet all of the key requirements of Section 522 for developing and implementing comprehensive privacy and data protection procedures. Specifically, the audit identified that FHFA had not:

- Completed a required privacy program baseline report summarizing FHFA's use of PII and establishing the control framework for privacy protection. The report was completed and submitted to FHFA-OIG after the conclusion of the audit field work in August 2011;
- Designed a job-specific privacy training program to ensure FHFA employees and contractors are familiar with privacy protection roles and responsibilities;
- Established a process for timely publication of required System of Record Notices that describe the existence and character of the system of records before operating systems containing PII;
- Prepared Privacy Impact Assessments of all systems that contain PII and documented assessments made of agency proposed rules to help ensure protection of PII was adequately considered in the systems development and rulemaking processes; and
- Implemented a process for FHFA's Privacy Office to monitor information systems containing PII after they are placed in production.

Addressing these control deficiencies in privacy and data protection procedures will strengthen FHFA's privacy program, further protect individuals from the adverse impact of breaches, and contribute to ongoing efforts to achieve reasonable assurance of adequate protection of PII.

Several of the recommendations made in this report relate to privacy practices that have not been incorporated into the Agency's policies and procedures. Absent formal policies and procedures, FHFA cannot ensure consistent privacy program implementation across all Agency operations and protection of the confidentiality, integrity, and availability of privacy information consistent with statutory and regulatory requirements.

TABLE OF CONTENTS

ABBREVIATIONS

CG ..... Clifton Gunderson

CPO ..... Chief Privacy Officer

CISO ..... Chief Information Security Officer

Fannie Mae ..... Federal National Mortgage Association

FHFA ..... Federal Housing Finance Agency

FHFA-OIG ..... Federal Housing Finance Agency Office of Inspector General

FHLBanks ..... Federal Home Loan Banks

Freddie Mac ..... Federal Home Loan Mortgage Corporation

FIPS ..... Federal Information Processing Standards

FISMA ..... Federal Information Security Management Act of 2002

GAGAS ..... Generally Accepted Government Auditing Standards

HERA ..... Housing and Economic Recovery Act of 2008

IT ..... Information Technology

NIST ..... National Institute of Standards and Technology

OMB ..... Office of Management and Budget

PII ..... Personally Identifiable Information

PIA ..... Privacy Impact Assessment

PTA ..... Privacy Threshold Analysis

Section 522 ..... Consolidated Appropriations Act of 2005

SSN ..... Social Security Number

SORN ..... System of Records Notice

Federal Housing Finance Agency

Office of Inspector General

Washington, DC

PREFACE

FHFA-OIG was established by the Housing and Economic Reform Act of 2008 (HERA),[1] which amended the Inspector General Act of 1978.[2] FHFA-OIG is authorized to conduct audits, investigations, and other activities of the programs and operations of FHFA; to recommend policies that promote economy and efficiency in the administration of such programs and operations; and to prevent and detect fraud and abuse in them. This is one in a series of audits, evaluations, and special reports published as part of FHFA-OIG's oversight responsibilities to promote economy, effectiveness, and efficiency in the administration of FHFA's programs.

The objective of this performance audit was to assess FHFA's privacy program and its implementation, including compliance with the statutory and regulatory requirements concerning the protection of PII. FHFA-OIG contracted with CG to conduct this statutorily required audit. CG's audit report is included in Appendix A of this report.

CG's audit report makes nine recommendations to FHFA to assist in strengthening its privacy program. FHFA-OIG adopts these recommendations and believes they will help the Agency achieve more economical, effective, and efficient operations. FHFA-OIG appreciates the assistance of all those who contributed to the audit.

This report has been distributed to Congress, OMB, and others and will be posted on FHFA-OIG's website, www.fhfaoig.gov/.

Russell A. Rau
Deputy Inspector General for Audits

[1] Public Law No. 110-289.

[2] Public Law No. 95-452.

APPENDIX A

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Privacy Program and Implementation – 2011, pages 1 – 34.

COUNT ON INSIGHT®

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Privacy Program and Implementation - 2011

Prepared for the
Federal Housing Finance Agency
Office of Inspector General

September 30, 2011

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.cliftoncpa.com

Table of Contents

Executive Summary

September 30, 2011

Honorable Steve A. Linick
Inspector General
Federal Housing Finance Agency
1625 Eye Street, NW
Washington, DC 20006

Dear Mr. Linick:

Section 522 of the Consolidated Appropriations Act of 2005, (Division H, Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005) (Section 522), as amended requires that each agency designate a Chief Privacy Officer (CPO) 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 relating to agency employees and the public. Section 522 also requires the Inspector General of each agency to periodically conduct a review of the agency's implementation of the requirements of Section 522 including the agency's privacy program. The Federal Housing Finance Agency (FHFA) Office of the Inspector General (FHFA-OIG) contracted with Clifton Gunderson (CG) to conduct a performance audit of FHFA's privacy program and its implementation. We are pleased to provide the Fiscal Year (FY) 2011 CG Independent Audit Report, detailing the results of our review of the FHFA's privacy program.

The objective of this performance audit was to assess FHFA's privacy program and its implementation, including compliance with the statutory and regulatory requirements concerning the protection of personally identifiable information (PII).[1] The specific sub-objectives were to determine whether FHFA implemented comprehensive privacy and data protection procedures as required by Section 522 and accurately reported on its use of information in an identifiable form, along with its privacy and data protection policies and procedures. CG's audit included a review of FHFA's privacy related policies and procedures, the structure and positioning of the Privacy Office's function within the agency, the monitoring and compliance efforts of the Privacy Office, and FHFA's network and website for privacy vulnerabilities. CG also reviewed the agency's privacy related training program. These areas were assessed accordingly within the context of the requirements and recommendations of Section 522, Section 208 of the E-Government Act of 2002, the Privacy Act of 1974, OMB memoranda M-03-22 and M-07-

[1] The terms "personally identifiable information" and "information in an identifiable form" are used interchangeably in privacy-related policies to describe information such as an individual's name, date of birth, and social security number. For purposes of this report, we use the term PII.

16, and NIST Special Publication (SP) 800-122. Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS).

While FHFA's privacy program had a number of strengths, such as a policy on the use and protection of PII, FHFA did not meet all of the key requirements of Section 522 for developing and implementing comprehensive privacy and data protection procedures. Specifically, the audit identified that FHFA had not:

- Completed a required privacy program baseline report summarizing FHFA's use of PII;[2]
- Designed the job-specific privacy training program to ensure FHFA employees and contractors are familiar with privacy protection roles and responsibilities;
- Established a process for timely publication of required System of Record Notices that describe the existence and character of the system of records before operating systems containing PII;
- Prepared Privacy Impact Assessments of all systems that contain PII and documented assessments made of agency proposed rules to help ensure protection of PII was adequately considered in the systems development and rulemaking processes; and
- Implemented a process for FHFA's Privacy Office to monitor information systems containing PII after they are placed in production.

Further, several of the recommendations made in this report relate to privacy practices that have not been incorporated into the agency's policies and procedures. Absent formal policies and procedures, FHFA cannot ensure consistent program implementation. In addition, there may be potential civil and criminal ramifications associated with noncompliance with laws if agency employees do not understand their responsibilities under the various privacy laws. FHFA is vulnerable to an increased risk of a breach of sensitive data, which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach. Addressing these control deficiencies in privacy and data protection procedures will strengthen FHFA's privacy program and contribute to ongoing efforts to achieve reasonable assurance of adequate protection of PII.

CG does not consider the findings in this report to be a significant deficiency as defined under the Federal Information Security Management Act of 2002 (FISMA).[3] However, CG concluded that collectively, the deficiencies are significant in the context of the audit objective as defined for performance audits under GAGAS.

FHFA's privacy program had a number of strengths, including but not limited to the following:

[2] On August 17, 2011, after completion of audit field work, FHFA provided the baseline report. FHFA-OIG will evaluate this report as part of future audits.

[3] See page 30 in this report for the definition of significant deficiency under FISMA and deficiency in internal control that is significant in the context of the audit objective according to GAGAS.

- The policy related to the use and protection of PII is documented and provides clear direction and guidance on the use of PII;
- The Breach Notification Policy is documented and roles and responsibilities are defined;
- The Privacy Office performs periodic walk-throughs of agency offices and work areas to monitor the physical protection of PII;
- The Privacy Office provides initial new hire and annual refresher privacy awareness training to all employees and contractors; and
- The Privacy Office oversees the performance of a Privacy Threshold Analysis (PTA) for all new information systems.

This report makes nine recommendations to assist FHFA in strengthening its privacy program.

This performance audit did not constitute an audit of financial statements in accordance with GAGAS. CG was not engaged to, and did not, render an opinion on the FHFA's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that controls may become inadequate because of changes in conditions, or because compliance with controls may deteriorate.

Sincerely,

Clifton Gunderson LLP

Clifton Gunderson LLP

Background

On July 30, 2008, FHFA was established by the Housing and Economic and Recovery Act of 2008 (HERA), Public Law No. 110-289. Specifically, HERA abolished two existing Federal agencies, the Office of Federal Housing Enterprise Oversight and the Federal Housing Finance Board, and in their place created FHFA to regulate the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), the 12 Federal Home Loan Banks (FHLBanks), and the Office of Finance. FHFA is an independent Federal agency, with a Director appointed by the President and confirmed by the U.S. Senate. Its mission is to provide effective supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac, and the FHLBanks. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the 12 FHLBanks. The Agency has a $201 million budget for fiscal year 2011 and a staff of 598.[4]

Section 522 of the Consolidated Appropriations Act, 2005

Public Law No. 108-447, Division H, Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 (commonly referred to as the Consolidated Appropriations Act of 2005) (Section 522), as amended,[5] states that each agency shall have a Chief Privacy Officer (CPO) to assume primary responsibility for privacy and data protection policy. According to Section 522, each agency shall prepare a written report of its use of information in an identifiable form,[6] along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Examples of information in identifiable form, also referred to as personally identifiable information (PII) include name, address, social security number (SSN) or other identifying number or code, telephone number, email address, etc. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report.

In addition, Section 522 requires the Inspector General of each agency to periodically conduct a review of the agency's implementation of the requirements of the section. The Inspector General may contract with an independent third party to conduct the review, to:

- Evaluate the agency's use of information in identifiable form;
- Evaluate the privacy and data protection procedures of the agency; and

[4] The Appendix, Other Independent Agencies, Budget of the United States Government, Fiscal Year 2012, http://www.whitehouse.gov/sites/default/files/omb/budget/fy2012/assets/oia.pdf, pp. 1239-1241.
[5] Section 522 as amended by Section 742 of the Consolidated Appropriations Act, 2008 (Public Law No. 110-161).
[6] The definition of "identifiable form" is consistent with the E-Government Act of 2002 (Public Law No. 101-347), and means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct of indirect means.

- Recommend strategies and specific steps to improve privacy and data protection management.

Per the requirements above, the independent third party review must also include:

- A review of the agency's technology, practices, and procedures with regard to the collection, use, sharing, disclosure, transfer, and storage of information in identifiable form;
- A review of the agency's stated privacy and data protection procedures with regard to the collection, use, sharing, disclosure, transfer, and security of personal information in identifiable form relating to agency employees and the public;
- A detailed analysis of agency intranet, network, and websites for privacy vulnerabilities, including:
  - Noncompliance with stated practices, procedures, and policies; and
  - Risks for inadvertent release of information in an identifiable form from the website of the agency; and
- A review of agency compliance with Section 522.

The Privacy Act of 1974

The Privacy Act of 1974, 5 U.S.C. § 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.

The information collected is considered a record under the Privacy Act if it is an item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

When an agency has a group of any records under its control from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, the agency has a system of records. The Privacy Act requires that a public notice, commonly referred to as a System of Records Notice (SORN), be published in the Federal Register that describes the existence and character of the system of records. In addition, the Privacy Act requires SORNs to include:

- The name and location of the system;
- The categories of individuals on whom records are maintained in the system;
- The categories of records maintained in the system;
- Each routine use of the records contained in the system, including the categories of users and the purpose of such use;

- The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
- The title and business address of the agency official who is responsible for the system of records;
- The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
- The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
- The categories of sources of records in the system.

E-Government Act of 2002

Section 208 of the E-Government Act of 2002 (Public Law No. 107-347) requires agencies to (1) conduct Privacy Impact Assessments (PIA) 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 Memorandum M-03-22

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* addresses privacy protections when members of the public interact with the Federal government and directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology to collect new information, or when agencies develop or buy new information technology (IT) systems to handle collections of PII. OMB Memorandum M-03-22 defines a PIA as an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. PIAs must analyze and describe the following:

- What information is to be collected (e.g., nature and source);
- Why the information is being collected (e.g., to determine eligibility);
- Intended use of the information (e.g., to verify existing data);
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- 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;
- How the information will be secured (e.g., administrative and technological controls); and
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. PIAs must also be approved by a "reviewing official" and be made publicly available to the extent that they do not contain classified or sensitive information or raise security concerns.

In addition to conducting PIAs, OMB Memorandum M-03-22 also requires agencies to post privacy policies on agency websites used by the public, translate privacy policies into a standardized machine-readable format, and report annually to OMB on compliance with Section 208 of the E-Government Act of 2002.

OMB Memorandum M-07-16

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB-M-07-16), requires agencies to develop and implement a breach notification policy and provides the framework within which agencies must develop this notification policy while ensuring proper safeguards are in place to protect the information. This memorandum also requires agencies to periodically review their holdings of PII and ensure that they are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of agency functions. OMB Memorandum M-07-16 also requires the agency to review the use of SSN and establish a plan to eliminate their unnecessary collection and use. There are also five security requirements within OMB Memorandum M-07-16:

- Encryption. Encrypt, using only National Institute of Standards and Technology (NIST)[7] certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and
- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities.

[7] NIST, an agency within the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

NIST Special Publication 800-122

NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* provides guidelines for implementing a risk-based approach to protecting PII in the context of information security. It recommends a process that involves identifying the PII that an agency holds, classifying the PII by confidentiality impact level, and providing safeguards based on the confidentiality impact level. It also provides recommendations for developing an incident response plan.

FHFA Privacy Office

The Privacy Office at FHFA is made up of two employees, the Privacy Officer and the Chief Privacy Officer (CPO) who has also been designated as the Senior Agency Official for Privacy and is responsible for ensuring compliance with federal laws, regulations, and policies related to information privacy. The Privacy Office has a policy in place for the protection of PII, *Use and Protection of Personally Identifiable Information*, as well as a policy for breach notification in the event of a privacy related incident, *Breach Notification Policy and Plan*. The agency has also compiled the *Privacy Threshold Analysis and Privacy Impact Assessment Guide* for use when performing Privacy Threshold Analyses (PTA) and PIAs described below.

FHFA Privacy Monitoring and Compliance

In addition to requiring a PTA for each new system as it moves through the system development life cycle, FHFA's policies also require a PTA if a modification to a system affects how the system uses, collects, or stores information. A PTA is a screening tool designed to assist the CPO in determining what privacy requirements apply to an information system. There are two parts to the PTA, the first is a questionnaire that is completed by the system owner that describes the nature and volume of information contained in the system. The second part, which is completed by the CPO, provides for the analysis of the system and the required next steps. A PTA collects the following information from the system owner in order to assist the CPO in determining what privacy requirements apply to a system:

- Name of the system and system owners;
- Status of the system, why the PTA is being performed;
- Does the system contain data fields that collect, maintain, or disseminate information on an individual(s)? If so, document the PII the system contains;
- Legal authority that allows FHFA to operate the system and collect the information;
- Name of SORN that covers the system, or notification that one does not exist;
- Whether the information in the system can be linked with other information to identify an individual;
- Nature of individuals the system contains information about;

- Whether the system collects data from 10 or more members of the public during a calendar year;
- The source of the information collected, and if from an individual is a Privacy Act Statement provided to the individual;
- Whether the information is retrieved by name of an individual or some identifying number, symbol, or other identifying particular assigned to the individual; and
- Whether a Certification and Accreditation has been performed, and if so, the Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, category (discussed below).

Based on the information provided by the system owners, the CPO performs an analysis of the system to determine whether:

- The system is a PII system;
- A new SORN is required for the system; and
- A Privacy Act Statement is required.

As part of the analysis, the CPO assigns a FIPS PUB 199 risk category to the information contained in the system to the extent it pertains to privacy. FIPS PUB 199 establishes security categories for information and information systems based on the potential impact on the agency should certain events occur which threaten the information and information systems needed by the agency. FISMA defines three security objectives for information and information systems:

Confidentiality - A loss of confidentiality is the unauthorized disclosure of information.

Integrity - A loss of integrity is the unauthorized modification or destruction of information.

Availability - A loss of availability is the disruption of access to or use of information or an information system.

The possible categories of potential impact are:

Low - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. FHFA PTAs use the wording, "The PII elements cannot be used to identify an individual or is normally publicly available."

Moderate - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. FHFA PTAs use the wording, "The PII elements are not normally publicly available, but do not pose a higher risk of subsequent identity theft or personal harm to the individual if released."

High - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. FHFA PTAs use the wording, "The PII elements are sensitive PII that pose a higher risk of subsequent identity theft or personal harm to the individual if released."

Based upon the analysis performed by the CPO as part of a PTA, a decision is made as to whether a PIA will be performed.[8] The degree of analysis within the PIA is dependent on the importance of the system and the FIPS PUB 199 category assigned to the privacy related data in the PTA. OMB Memorandum M-03-22 defines a major system as a system or project that requires special management attention because of its:

1. Importance to the agency mission;
2. High development, operating, and maintenance costs;
3. High risk;
4. High return; and
5. Significant role in the administration of an agency's programs, finances, property or other resources.

According to OMB Memorandum M-03-22, a PIA conducted for a major system should reflect extensive analyses of the:

1. Consequences of collection and flow of information;
2. Alternatives to collection and handling as designed;
3. Appropriate measure to mitigate risks identified for each alternative; and
4. Rationale for the final design choice or business process.

In addition, OMB Memorandum M-03-22 states that the depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.

The PIA documents how the information collected within a system is used and the safeguards in place to protect that information. The system owner completes the PIA with input and approval from the system developer, the Chief Information Security Officer, the Chief Information Officer, and the CPO.

The Privacy Office also performs periodic examinations of the FHFA offices to assess compliance with privacy policies.

FHFA Privacy Awareness and Training

FHFA's Privacy Office provides initial new hire and annual refresher privacy training to all employees and contractors. The training is delivered through the assigned FHFA computer and is administered in conjunction with other IT related training. If an

[8] See the section above title OMB Memorandum M-03-22 for a discussion of PIAs.

employee/contractor has not completed the required privacy training within a reasonable period of time, the CPO will have that employee's/contractor's access to FHFA's information systems turned off until the training is completed.

Results of Audit

Overview

Section 522 requires an agency to designate a CPO 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 relating to agency employees and the public.

A comprehensive privacy program helps to ensure that risks related to the collection, storage, transmission and destruction of PII are mitigated. A strong privacy program also provides a framework for the agency to consider the implications of business decisions made as they pertain to PII. A privacy program should also help maintain public trust and confidence in an organization, protect the reputation of an organization, and protect against legal liability for an organization by providing the necessary safeguards to minimize the risk of unintended disclosure of PII.

CG's audit included a review of FHFA's privacy related policies and procedures, the structure and positioning of the Privacy Office's function within the agency, the monitoring and compliance efforts of the Privacy Office, and FHFA's network and website for privacy vulnerabilities. CG also reviewed the agency's privacy related training program. These areas were assessed within the context of the requirements and recommendations of Section 522, Section 208 of the E-Government Act of 2002, the Privacy Act of 1974, OMB memoranda M-03-22 and M-07-16, and NIST SP 800-122.

While FHFA's privacy program had a number of strengths, such as a policy on the use and protection of PII, FHFA did not meet all of the key requirements of Section 522 for developing and implementing comprehensive privacy and data protection procedures. Specifically, the audit identified that FHFA had not:

- Completed a required privacy program baseline report summarizing FHFA's use of PII;[9]
- Designed the job-specific privacy training program to ensure FHFA employees and contractors are familiar with privacy protection roles and responsibilities;
- Established a process for timely publication of required SORNs that describe the existence and character of the system of records before operating systems containing PII;
- Prepared PIAs of all systems that contain PII and documented assessments made of agency proposed rules to help ensure protection of PII was adequately considered in the systems development and rulemaking processes; and
- Implemented a process for FHFA's Privacy Office to monitor information systems containing PII after they are placed in production.

[9] Id. at page 4.

Further, several of the recommendations made in this report relate to privacy practices that have not been incorporated into the Agency's policies and procedures. Absent formalized practices, FHFA cannot ensure consistent program implementation. In addition, there may be potential civil and criminal legal ramifications associated with noncompliance with laws if agency employees do not understand their responsibilities under the various privacy laws. FHFA is vulnerable to an increased risk of a breach of sensitive data, which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach. Addressing these control deficiencies in privacy and data protection procedures will strengthen FHFA's privacy program and contribute to ongoing efforts to achieve reasonable assurance of adequate protection of information in an identifiable form.

CG does not consider the five findings stated in this report to be a significant deficiency as defined under FISMA.[10] However, CG concluded that collectively, the deficiencies are significant in the context of the audit objective as defined for performance audits under GAGAS.

Appendix II (page 32) of this report summarizes the results of testing performed of key criteria selected for evaluation associated with FHFA's privacy program and its implementation. Our detailed findings are discussed on pages 16-25.

[10] See page 30 in this report for the definition of significant deficiency under FISMA.

Finding 1. FHFA Needed to File the Baseline Report with the FHFA-OIG in a Timely Manner

FHFA did not file a baseline report required by Section 522 with FHFA-OIG in a timely manner. The Inspector General was sworn in to office on October 12, 2010, and the report was not filed until August 17, 2011. The report was filed after the completion of audit field work and was not subject to review by CG.

Section 522 states:

> (a) PRIVACY OFFICER- Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:
>
> (c) RECORDING- Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report.

FHFA-OIG was established at FHFA in October 2010. The baseline report was not filed by the Agency due to the time required to gather the information to prepare the report. Without a baseline report, FHFA lacks assurance of compliance with established privacy policies.

The baseline report serves as a useful benchmark for the agency's privacy program. Without proper documentation of the privacy policies and procedures within the FHFA baseline report, users may not be aware of FHFA's policies and procedures relating to the privacy and data protection of PII, and will not be able to measure actual privacy and data protection practices against the agency's recorded privacy and data protection policies. As a result, employees may rely on undocumented practices that may not be in accordance with the appropriate legal or regulatory guidance and employees may mishandle PII exposing the agency to a breach or compromise of PII.

With submission of the baseline report by the Agency, this finding contains no recommendations, and no further action is necessary. However, FHFA-OIG will evaluate the baseline report as part of future audits.

Finding 2. FHFA Needs to Strengthen the Privacy Training Program

Although recommended by NIST SP 800-122, FHFA has not documented a privacy training plan and implementation. Also, FHFA has not identified employees that would benefit from additional job-specific or role based training based on increased responsibilities related to PII, and a specific role based training program has not been developed or implemented. OMB M-07-16 requires privacy related training to be job-specific and commensurate with employee's responsibilities. In addition, NIST SP 800-122 specifies role-based training be provided depending on the roles and functions involving PII.

A job-specific privacy training program is important for FHFA to implement as violations of the Privacy Act and OMB Memorandum M-03-22 with regard to SORNs and PIAs were noted. For example, two systems of records were in place prior to the publication of their respective SORNs, and PIAs were not completed for four systems containing PII (refer to findings 3 and 4, pages 20 and 22, respectively).

OMB Memorandum M-07-16 states:

> Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities.
>
> Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.
>
> Fairness requires that managers, supervisors and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities. Consequences should be commensurate with level of responsibility and type of personally identifiable information involved. Supervisors also must be reminded of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information. Agencies should develop and implement these policies in accordance with the agency's respective existing authorities.

NIST SP 800-122 states:

> An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. Organizational policy should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training periodicity and refresher training requirements. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training. Depending on the roles and functions involving PII, important topics to address may include:

- The definition of PII
- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents and reporting.

Education through training develops a common body of knowledge that reflects all of the various specialties and aspects of PII protection. It is used to develop privacy professionals who are able to implement privacy programs that enable their organizations to proactively respond to privacy challenges

Although FHFA provides new hire and annual refresher training related to privacy, the training program does not specifically address the need for additional or advanced training for those individuals with increased responsibilities related to PII. FHFA has not completed an analysis of the roles within the agency with increased levels of responsibilities related to PII.

FHFA has documented privacy policies and procedures in its *Use and Protection of Personally Identifiable Information Policy*. However, a privacy training plan and implementation approach has not been prepared.

Training programs reinforce the execution of the privacy policies and decrease the risk of privacy incidents. Additional or advanced training should be provided to those individuals with increased privacy management responsibilities such as Privacy Office employees and managers who handle PII to remind them to keep in mind privacy controls when making decisions involving the collection, use, sharing, retention, disclosure, and destruction of PII. Without role based training, individuals may not be fully aware of privacy protection requirements specific to the data and records they process.

Privacy training is designed to reinforce employees' understanding of privacy risk management processes such as restrictions on data collection, storage, and use of PII. While FHFA may have effective practices in place based on the institutional knowledge of the CPO, absence of a documented training plan and implementation approach may lead to inadequate or inconsistent training and a lack of understanding of practices for adequate protection of PII. Ultimately, FHFA is vulnerable to an increased risk of a breach of sensitive data, which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach.

We recommend that FHFA's CPO:

Recommendation #1. Document, disseminate, and implement a privacy training plan and implementation approach.

Recommendation #2. Identify those employees that would benefit from additional job specific or role-based privacy training based on increased responsibilities related to PII.

Recommendation #3. Develop and implement targeted role based training for employees whose job functions require additional job specific or role based privacy training.

Finding 3. FHFA Needs to Ensure System of Record Notices are Published Prior to Systems Being Placed in Operation.

Of the 18 systems of records reviewed, FHFA had two systems, "mail, contact, phone and other lists;" and "freedom of information and privacy act records," in place prior to the publication of their respective system-specific SORNs. The Agency believed that all records within the systems were in fact part of one system. However, upon further review it was determined that the systems were in fact distinct and warranted separate SORNs. While FHFA had published a general SORN to cover these types of records, not publishing more specific SORNs prior to creating new systems of records could lead to a violation of the Privacy Act. These systems are end user computer and paper based systems that contain PII.

***The Privacy Act of 1974* states:**

> A public notice is required to be published:
>
> For new systems, before the system of records becomes operational; i.e., before any information about individuals is collected,

The "mail, contact, phone and other lists" system was created by the Office of Communications (OC) to track inquiries made by the public. The OC was not aware of their responsibility to prepare a SORN prior to creating the system.

The "freedom of information and privacy act records" system was created by the previous Freedom of Information Act (FOIA) officer who concluded that it did not constitute a system of records under the Privacy Act. When the CPO became the FOIA Officer, he determined that it was in fact a system of record and published the required SORN.

Since these systems are end user computer and paper based systems, they were not subject to the formal certification and accreditation process that would have identified the need for a SORN. Without a process in place for identification and monitoring of the creation of end user computer and paper based systems, the Agency and the CPO may not be aware that such systems exist.

A SORN is completed during the *Requirements Analysis Phase* and the *Design Phase* of the system development life cycle process by the respective project manager. This notice describes the system of record and gives the public an opportunity to provide their views and comments in line with the Privacy Act provisions. The lack of publishing a SORN prior to a system being operational may lead to individuals not understanding the privacy risks associated with the system, what information is being collected about them, or their rights related to review of the information collected. There are also potential civil and criminal legal ramifications related to operating and maintaining systems of records without publishing the required notices.

We recommend that FHFA's CPO:

Recommendation #4. Develop and implement additional training for employees about SORN requirements, focusing on the inadvertent creation of systems of records. This training should stress the legal ramifications potentially associated with creating systems of records prior to publishing a SORN.

Recommendation #5. Strengthen its privacy related procedures to ensure SORNs are completed prior to systems becoming operational.

Finding 4. FHFA Needs to Prepare Privacy Impact Assessments of all Systems that Contain PII and Document Assessments Made of Agency Proposed Rules

Although required by OMB Memorandum M-03-22, Privacy Impact Assessments (PIA) were not completed by system owners for four systems containing PII. The systems are: Trakker, Affordable Housing Program/Community Investment Cash Advance (AHP/CICA), Content Management Interface (CMI), and Office of Conservatorship Operations' (OCO) Status Report Tracking System. OMB Memorandum M-03-22 allows for a simplified PIA utilizing checklists or templates to be performed, but one must still be completed. In addition, the Privacy Office has not documented assessments required by section 522 of proposed rules of the Agency as it relates to privacy of information in an identifiable form.

OMB Memorandum M-03-22 states:

> *Privacy Impact Assessment (PIA)*- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
>
> The E-Government Act of 2002 (Public Law No. 107-347) requires agencies to conduct a PIA before:
>
> Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public.
>
> The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
>
> Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.

Section 522 states:

> (a) PRIVACY OFFICER- Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:
>
> (5) conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected;

According to the CPO, he made the decision that a PIA need not be performed by system owners for the four systems because they only contained one or two pieces of PII, usually a name or email address. In addition, the CPO asserted that the reviews of Agency proposed rules were conducted on an informal basis between the CPO and

those developing the proposed rules; however, the assessments were not documented and therefore, could not be substantiated.

Without completing a PIA on a system with PII, the Agency may face a potential loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of PII, which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach of PII. In addition, if a privacy impact assessment is not performed on proposed rules, FHFA may collect new information or change the way that information is used that would increase the privacy risks to the Agency.

We recommend that FHFA's CPO:

Recommendation #6. Require the system owners of the following systems with PII to prepare a PIA utilizing a template or checklist: Trakker, AHP/CICA, CMI, and OCO Status Report Tracking System.

Recommendation #7. Document the privacy impact assessments conducted for proposed rules of the Agency as required by Section 522.

Recommendation #8. Establish a process for the completion of template or checklist based PIAs and modify policies and procedures as necessary.

Finding 5. FHFA Needs to Document, Disseminate, and Implement a Process to Monitor Information Systems Containing PII After being Placed in Production

FHFA's Privacy Office has not identified and documented the privacy related security controls that must be monitored for information systems containing PII that have been placed in the production environment, and how the results of that monitoring should be communicated to the Privacy Office on an ongoing basis.

Section 522 states:

> (a) PRIVACY OFFICER- Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:
>
> (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;
>
> (7) ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

Federal Housing Finance Agency Program Management Procedures in line with NIST SP 800-53 Rev. 3 states:

> Continuous Monitoring - (CA-7)
>
> By regularly reviewing the effectiveness of security controls within FHFA information systems, Program Offices/System Owners are able to quickly detect and respond to new vulnerabilities.

Although system tools are implemented for logging, there is no process in place for CPO review of the logs, and no documented process for monitoring other privacy related security controls, therefore monitoring is not fully implemented.

Business processes and systems in production from time to time go through changes that may introduce privacy risks. Changes may significantly alter system information and may require additional controls to protect any PII they contain. Lack of monitoring of information systems containing PII after they are placed in production may lead to a compromise or breach of PII especially when conditions of systems change, i.e., a system is modified or used for a purpose other than what it was originally designed for.

We recommend that that FHFA's CPO, in coordination with the Chief Information Security Officer (CISO):

Recommendation #9. Ensure privacy risk is continuously assessed on systems in production, including when functionalities change or when a major update is done. The CPO should document, disseminate (to system owners and the CISO), and implement policies and procedures for continuous monitoring of information systems containing PII after they are placed in production. The policies and procedures at a minimum should:

a. Document the privacy related security controls that are to be monitored to protect information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;
b. Determine the frequency of the privacy related security controls monitoring and reporting process to the Privacy Office;
c. Document review of reports generated by the monitoring of the privacy related security controls noted in item b. above; and
d. If necessary, take action on results of monitoring and document results of action taken.

Appendix I – Objective, Scope, and Methodology

Objective

The objective of this performance audit was to assess FHFA's privacy program and its implementation, including compliance with the statutory and regulatory requirements concerning the protection of PII. The specific sub-objectives were to determine whether FHFA implemented comprehensive privacy and data protection procedures as required by the Section 522, as amended and accurately reported on its use of information in an identifiable form, along with its privacy and data protection policies and procedures.

Scope

In assessing FHFA's compliance with the requirements of Section 522, CG evaluated the following areas:

- FHFA's Privacy Policies and Procedures,
- FHFA's Privacy Office,
- FHFA's Privacy Monitoring and Compliance (included evaluation of PIAs and SORNs),
- Privacy vulnerability analysis of FHFA's network and website, and
- Privacy Awareness and Training.

During the audit, CG performed a review of the following documentation provided by the FHFA:

- Use and Protection of Personally Identifiable Information Policy,
- Breach Notification Policy and Plan,
- Privacy Threshold Analysis and Privacy Impact Assessment Guide,
- Privacy Office Organizational Chart,
- Chief Privacy Officer Designation,
- Draft SORN Guidance Document,
- Draft Baseline Report,
- FY 2011 Privacy Plan to Reduce PII and SSNs,
- Inventory of IT Systems with Personally Identifiable Information, and
- New Hire Training Program.

Methodology

1. Review of FHFA's Privacy Policies and Procedures

According to Section 522, each agency is required 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 relating to the agency employees and the public. Such procedures

shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and Section 208 of the E-Government Act of 2002.

CG performed a thorough review of FHFA's policy documentation to assess adherence to Section 522. CG reviewed FHFA's baseline privacy documentation. In assessing the privacy policies and procedures, CG determined compliance with federal guidelines related to privacy and protection of personal identifiable information.

2. Review of FHFA's Privacy Office

Section 522 also requires that each Agency designate a CPO to assume primary responsibility for privacy and data protection policy. CG performed a review of FHFA's Privacy Office to determine whether the office effectively and efficiently administered FHFA's privacy program. In assessing the Privacy Office, CG reviewed the agency's organization charts/structure and interviewed key privacy officials to determine whether the Agency has identified roles and responsibilities for key privacy officials. In addition, CG reviewed the appointment letter and job description for the CPO to determine overall roles and responsibilities. CG also interviewed the CPO to determine if he was performing all responsibilities and had sufficient resources to perform his duties. In addition, CG determined whether the Privacy Office established processes for ensuring agency compliance with Federal and agency privacy policies. CG also determined whether the Privacy Office implemented procedures in identifying and securing information systems containing PII.

3. Review of FHFA's Privacy Monitoring and Compliance

During this audit, CG performed procedures to determine whether the Privacy Office effectively and efficiently administers FHFA's privacy program. To accomplish this objective, CG:

- Determined whether FHFA identified and maintained a complete inventory of information systems containing PII and systems requiring PIAs and has conducted PIAs for the information systems. The inventory provided lists 26 systems noted as containing PII.

- For a sample of five information systems, CG reviewed the PIAs and determined whether these PIAs have, at a minimum, analyzed and described:
    - What information needs to be collected (e.g., nature and source);
    - Why the information is being collected (e.g., to determine eligibility);
    - Intended use of the information (e.g., to verify data);
    - With whom the information will be shared (e.g., another agency for a specified programmatic purpose);
    - Opportunities individuals have to decline to provide information (e.g., 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; and

  - How the information will be secured (e.g., administrative and technological controls).

- CG reviewed PIAs and related documentation for the following systems:
  - Examiner Workstation,
  - Web-TA,
  - HSPD-12 PIV,
  - e-OPF, and
  - Litigation Support System.

- In addition, CG performed procedures to determine whether a SORN was required and if required, whether one was published. CG reviewed FHFA's publication of SORNs in the Federal Register and verified that they contain only information about individuals that was "relevant and necessary" to accomplish FHFA's mission. In addition, CG determined whether SORNs have been updated to reflect the Agency's current systems of records.

- Furthermore, consistent with guidance issued by OMB in 2007 related to privacy protection (OMB Memorandum M-07-16), CG reviewed procedures implemented by FHFA to ensure:

  - Privacy was adequately protected and FHFA management has implemented breach notification policies;
  - Procedures were in place to reduce the use of SSNs;
  - Policies existed to notify external agencies about privacy breaches; and
  - FHFA has implemented policies for consequences and accountability for privacy violation.

4. Privacy Vulnerability Analysis

CG performed a thorough review and analysis of FHFA's network and its external website for privacy vulnerabilities in accordance with Section 522. These privacy vulnerabilities include noncompliance with stated practices, policies and procedures as well as risks of inadvertent release of information in an identifiable form from the website of the Agency.

In completing the vulnerability analysis, the first task was to review results from vulnerability assessments conducted during FY 2011 to determine the scope of the review and whether any privacy related vulnerabilities were identified as a result of the assessments. The objective was to determine whether any vulnerabilities were identified on the FHFA network related to the risk of inadvertent release of information in an identifiable form from the Agency's network.

In addition, CG gained a thorough understanding of the FHFA's documented standards regarding its system's handling and tracking of PII. Once the CG team had a thorough understanding of the agency's policies as well as its approach to privacy compliance,

the team worked with the appropriate FHFA personnel to test and document the application of selected privacy related technical controls from NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*, within FHFA's network. Technical controls tested include but were not limited to:

- Access Control
  - Access Enforcement – AC -1
  - Remote Access – AC-17
- Planning
  - Privacy Impact Assessment – PL-5
- System and Communications Protection
  - System and Communication Protection Policy and Procedures – SC-1
  - Information in Shared Resources - SC-4
  - Boundary Protection - SC-7
  - Transmission Integrity - SC-8
  - Transmission Confidentiality - SC-9
  - Public Access Protections - SC-14
  - Public Key Infrastructure Certificates - SC-17
- System and Information Integrity
  - Software and Information Integrity – SI-7

CG tested to determine if the Agency has implemented encryption on data transmitted over the agency's communication infrastructure with emphasis on encryption of systems containing privacy data. Our testing enabled us to determine if the information transmitting across the network boundaries is secure and identify any control weaknesses with respect to PII.

In order to conduct the website testing discussed above CG performed procedures to determine the following for the website:

- Whether the website was using Secure Socket Layer (SSL) to capture and transfer Privacy Act protected user data;
- Whether the appropriate privacy policy and disclosures were posted and available for all visitors and users of the website (CG assessed the web privacy policies to ensure they have implemented the requirements set forth in OMB Memorandum M-03-22, Section III - *Privacy Policies on Agency Websites*, and FHFA Privacy Policies.);
- Whether the website was in compliance with the use of tracking mechanisms;
- Ensure that any personal identifiable information was protected; and
- Whether FHFA has implemented machine readability technology on its public website, such as Privacy Preferences Project Protocol (P3P).

5. Review of FHFA's Privacy Awareness and Training

During this task, CG performed procedures to determine whether the Agency has established privacy training requirements in accordance with Federal and Agency

guidance. In addition, CG determined whether FHFA has implemented a training program regarding role based training for individuals responsible for PII. CG documented whether specific user roles have been identified by FHFA that require role-based training.

CG conducted this audit in accordance with GAGAS issued by the Comptroller General of the United States. Those standards require that audits be planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objective. CG believes that the evidence obtained provides a reasonable basis for the findings and conclusions included herein, based on the audit objective.

To assist in the audit, CG reviewed prior year reports to identify potential risk areas. The prior year reports CG reviewed include the FHFA's FY 2010 Federal Information Security Act (FISMA) evaluation[11] and FY 2009 independent audit report on privacy and data protection.[12] CG also reviewed a Government Accountability Office (GAO) report on opportunities for improving FHFA's internal controls and accounting procedures,[13] GAO's report on opportunities for improving information system controls,[14] and GAO's financial audit report for FHFA's FY 2009 and FY 2010 financial statements.[15] Additionally, CG reviewed FHFA's policies, procedures and records and conducted interviews of FHFA employees and contractor personnel.

A significant deficiency under FISMA is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. As required in FISMA (Section 3544(c)(3)), agencies are to report any significant deficiency in policy, procedure, or practice as a material weakness in reporting under the Federal Managers' Financial Integrity Act and if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act.

CG does not consider the deficiencies noted in this report to be a significant deficiency under FISMA. However, CG concluded collectively that the deficiencies are significant in context of the audit objective as defined for performance audits under GAGAS.

---

[11] *Federal Housing Finance Agency Fiscal Year 2010 Independent Auditor's Federal Information Security Management Act (FISMA) Report,* FHFA Audit Report No. 10-A-03-0TIM, September 30, 2010

[12] *FY 2009 Independent Audit Report on Privacy and Data Protection*, Audit Report No. 09-A-01-OCAO/OTIM

13 Management Report: Opportunities for Improvement in the Federal Housing Finance Agency's Internal Controls and Accounting Procedures, GAO-11-398R, April 29, 2011

[14] *Information Security: Opportunities Exist for the Federal Housing Finance Agency to Improve Controls*, GAO-10-528, April 2010

[15] *Financial Audit: Federal Housing Finance Agency's Fiscal Years 2010 and 2009 Financial Statements*, GAO-11-151, November 2010

According to these standards,[16] significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives.

[16] Paragraph 7.04, Significance in a Performance Audit, GAO-07-731G (07/07), p. 123.

Appendix II – Summary of Key Criteria Tested

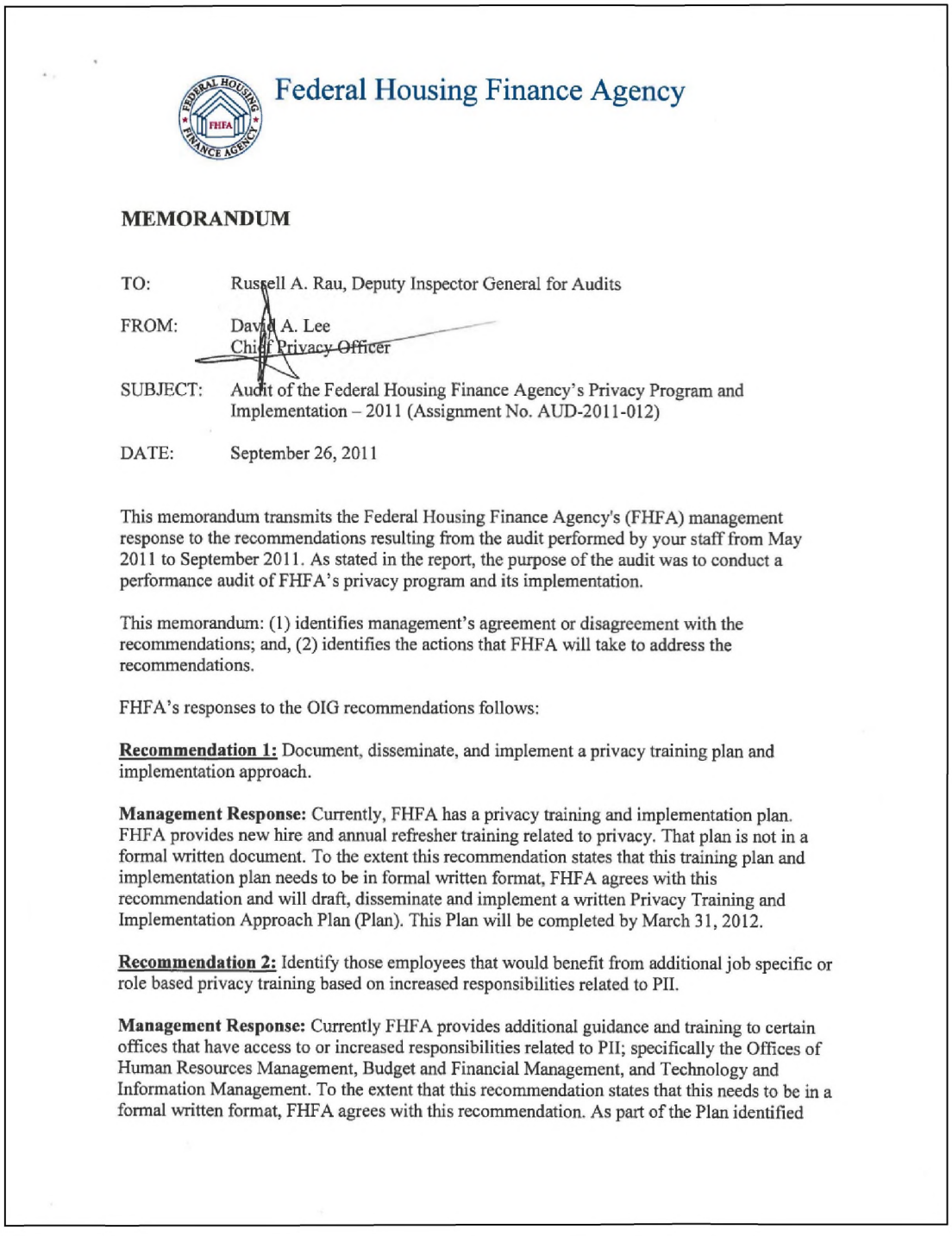
	Policy Requirement	Audit Conclusion
1	**Sec 522 of the 2005 Appropriations Act**	
1.a	Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form	Issue noted. See Recommendation #6 and #8.
1.b	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	Issue noted. See Recommendation #9.
1.c	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	Issue noted. See Recommendation #4 and #5.
1.d	Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government	No issues noted.
1.e	Conducting a privacy impact assessment of proposed rules of the department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected	Issue noted. See Recommendation #7.
1.f	Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementations of section 552a of title 5, 11 United States Code, internal controls and other relevant matters	No issues noted.
1.g	Ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction	Issue noted. See Recommendation #9.
1.h	Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies	Issue noted. See Recommendation #1, #2, and #3.
1.i	Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency	Issue noted. See Finding #1.

	Policy Requirement	Audit Conclusion
2	**OMB M-07-16**	
2.a	Review and Reduce the volume of PII	No issues noted.
2.b	Reduce the Use of Social Security Numbers	No issues noted.
2.c	Encrypt all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing.	No issues noted.
2.d	Allow remote access only with two factor authentication where one of the factors is provided by a device separate from the computer gaining access	No issues noted.
2.e	Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity	No issues noted.
2.f	Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required	No issues noted.
2.g	Implement procedures for detecting, reporting and responding to security incidents	No issues noted.
2.h	Rules and consequences policy	No issues noted.
3	**OMB M-03-22**	
3.a	Conduct PIAs for electronic information systems and collections and, in general, make them publicly available	Issue noted. See Recommendation #6 and #8. PIAs are publicly available.
3.b	Post privacy policies on agency websites used by the public	No issues noted.
3.c	Translate privacy policies into a standard machine-readable format	No issues noted.
3.d	Report annually to OMB on compliance with section 208 of the E-Government Act	No issues noted.
4	**Privacy Act of 1974**	
4.a	Publication of SORNs	Issue noted. See recommendation #4 and #5.
4.b	Identify each system of records which the agency maintains	No issues noted.
4.c	Establish reasonable administrative, technical and physical safeguards to assure that records are disclosed only to those who are authorized to have access	No issues noted related to administrative and physical safeguards. Issue noted for technical safeguard monitoring. See recommendation #9.
4.d	Review all agency contracts which provide for the maintenance of systems of records by or on behalf of the agency to assure that language is included which provide that such systems will be maintained in a manner consistent with the Act	No issues noted.
5	**NIST 800-122**	

	Policy Requirement	**Audit Conclusion**
5.a	Impact Level Definitions	No issues noted.
5.b	Awareness, Training, and Education	Issue noted. See Recommendation #1, #2, #3.
5.c	Security Controls	No issues noted.

APPENDIX B

FHFA's Comments to FHFA-OIG's Draft Report



Federal Housing Finance Agency

MEMORANDUM

TO: Russell A. Rau, Deputy Inspector General for Audits

FROM: David A. Lee
Chief Privacy Officer

SUBJECT: Audit of the Federal Housing Finance Agency's Privacy Program and Implementation – 2011 (Assignment No. AUD-2011-012)

DATE: September 26, 2011

This memorandum transmits the Federal Housing Finance Agency's (FHFA) management response to the recommendations resulting from the audit performed by your staff from May 2011 to September 2011. As stated in the report, the purpose of the audit was to conduct a performance audit of FHFA's privacy program and its implementation.

This memorandum: (1) identifies management's agreement or disagreement with the recommendations; and, (2) identifies the actions that FHFA will take to address the recommendations.

FHFA's responses to the OIG recommendations follows:

Recommendation 1: Document, disseminate, and implement a privacy training plan and implementation approach.

Management Response: Currently, FHFA has a privacy training and implementation plan. FHFA provides new hire and annual refresher training related to privacy. That plan is not in a formal written document. To the extent this recommendation states that this training plan and implementation plan needs to be in formal written format, FHFA agrees with this recommendation and will draft, disseminate and implement a written Privacy Training and Implementation Approach Plan (Plan). This Plan will be completed by March 31, 2012.

Recommendation 2: Identify those employees that would benefit from additional job specific or role based privacy training based on increased responsibilities related to PII.

Management Response: Currently FHFA provides additional guidance and training to certain offices that have access to or increased responsibilities related to PII; specifically the Offices of Human Resources Management, Budget and Financial Management, and Technology and Information Management. To the extent that this recommendation states that this needs to be in a formal written format, FHFA agrees with this recommendation. As part of the Plan identified

above in Recommendation 1, FHFA will identify those employees or offices that would benefit from additional job specific or role based privacy training based on increased responsibilities related to PII. This will be completed by March 31, 2012.

Recommendation 3: Develop and implement targeted role based training for employees whose job functions require additional job specific or role-based privacy training.

Management Response: Currently FHFA provides additional guidance and training to certain offices that have access to or increased responsibilities related to PII; specifically the Offices of Human Resources Management, Budget and Financial Management, and Technology and Information Management. To the extent that this recommendation states that this needs to be in a formal written format, FHFA agrees with this recommendation. As part of the Plan identified above, FHFA will identify those employees or offices that would benefit from additional job specific or role based privacy training based on increased responsibilities related to PII. In addition, targeted role based training will be developed and implemented. The Plan will be completed by March 31, 2012, and the targeted training will be completed by May 31, 2012.

Recommendation 4: Develop and implement additional training for employees about SORN requirements, focusing on the inadvertent creation of systems of records. This training should stress the legal ramifications potentially associated with creating systems of records prior to publishing a SORN.

Management Response: FHFA agrees that training employees is crucial to having a comprehensive privacy and data protection program. As part of the Plan identified above, FHFA will develop and implement training for employees on when and why SORNs are required and how to draft them to meet Privacy Act requirements. This Plan will be completed by March 31, 2012. New employee training already includes information regarding SORNs, however, the training will be updated to place greater emphasis on the requirements of the Privacy Act as it relates to systems of records. This new training will be incorporated into new employee and annual Privacy Awareness training during fiscal year 2012.

Recommendation 5: Strengthen its privacy related procedures to ensure SORNs are completed prior to systems becoming operational.

Management Response: FHFA agrees that strong privacy related procedures are important to having a comprehensive privacy and data protection program. A "Procedure on How and When to Draft a Privacy Act System of Records Notice" is currently in draft form. This document will address when and why SORNs are required and how to draft one to meet Privacy Act requirements. This document will be posted to the FHFA Info Site by November 30, 2011, and will form the basis for training employees on SORNs.

Recommendation 6: Require the system owners of the following systems with PII to prepare a PIA utilizing a template or checklist: Trakker, AHP/CICA, CMI, and OCO Status Report Tracking System.

Management Response: These following systems contain PII.

- Trakker = Name
- AHP/CICA = Address (The address information reported can be for various projects including single family or multi-family projects and can be in varying detail (e.g. street address, zip code only, city only, etc.). However, the FHLBanks do not report the address of individual households to FHFA.
- CMI = Email address
- OCO Status Report Tracking System = Name and business email

The e-Government Act of 2002 (Public Law No. 107-347) states that the depth and content of a Privacy Impact Assessment (PIA) should be appropriate for the nature of the information collected and the size and complexity of the IT system. Further, OMB Memorandum 03-22 states that for routine database systems, an agency may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.

None of the data collected in the four identified systems (name, email, and address (in the format described above)) is considered sensitive PII. Rather, the nature of the information collected in these four systems is routine, with limited use and access. In analyzing these systems, FHFA has utilized a standard approach whereby the Privacy Threshold Analysis (PTA) contains a checklist which satisfies the requirement to conduct a PIA on routine database systems.

FHFA currently has posted on its Info Site a Privacy Threshold Analysis and Privacy Assessment Guide. Nevertheless, to improve upon FHFA's review of these and other similar systems, FHFA will update the Privacy Threshold Analysis and Privacy Impact Assessment Guide to address how routine database systems containing routine information with limited use and access are analyzed. In addition, FHFA will update the PTA form to include a section that clearly identifies those systems that are "routine database systems." The form will also include a section where the individual conducting the analysis indicates that an analysis was conducted and will include the following elements:

- The system was identified as a routine database system,
- the information collected is non-sensitive PII, and
- the PTA meets the requirements of conducting a PIA on simple systems containing routine information and involving limited use and access.

These updates will be completed by January 31, 2012.

Recommendation 7: Document the privacy impact assessments conducted for proposed rules of the Agency as required by Section 522.

Management Response: FHFA agrees with this recommendation and will draft agency-wide guidance on how and when such assessments will be conducted on proposed regulations. This guidance will require coordination with all FHFA Divisions and Offices. Consequently this is expected to be completed by September 28, 2012.

Recommendation 8: Establish a process for the completion of template or checklist based PIAs and modify policies and procedures as necessary.

Management Response: See response to Recommendation 6.

Recommendation 9: We recommend that that FHFA's CPO, in coordination with the Chief Information Security Officer: Ensure privacy risk is continuously assessed on systems in production, including when functionalities change or when a major update is done. The CPO should document, disseminate (to system owners and the CISO), and implement policies and procedures for continuous monitoring of information systems containing PII after they are placed in production. The policies and procedures at a minimum should:

a. Document the privacy related security controls that are to be monitored to protect information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;
b. Determine the frequency of the privacy related security controls monitoring and reporting process to the Privacy Office;
c. Document review of reports generated by the monitoring of the privacy related security controls noted in b. above; and
d. If necessary, take action on results of monitoring and document results of action taken.

Management Response: FHFA agrees with this recommendation. The CPO will work with the CISO and system owners to draft and implement written policies and procedures for continuous monitoring of information systems containing PII. FHFA will develop an agency-wide process for continuous monitoring of information systems containing PII. This policy will require coordination with all FHFA Divisions and Offices and is expected to be completed by September 28, 2012.

If you have any questions, please contact me at (202) 414-3804, or david.lee@fhfa.gov.

APPENDIX C

FHFA-OIG's Response to FHFA's Comments

On September 26, 2011, FHFA provided a response (Appendix B) to the draft of this report. FHFA concurred with all recommendations made and described actions it plans to take or has taken to address the issues identified in the report (Appendix A). Based on FHFA's response, FHFA-OIG considers the actions sufficient to resolve the recommendations. However, the recommendations will remain open until such time as FHFA-OIG determines that agreed upon corrective actions are completed and responsive. See Appendix D of this report for a summary of management's comments on the recommendations.

With regard to recommendation six, FHFA proposed alternate corrective actions to improve upon FHFA's review of four systems—where PIAs were not completed by the system owners—and other similar systems. FHFA-OIG believes the Agency's actions—which includes updates to its *Privacy Threshold Analysis and Privacy Impact Guide* and PTA form to address "routine database systems"—meets the intent of the recommendation. Specifically, the PTA form will be updated to include the following elements:

- The system was identified as a routine database systems;
- The information collected is non-sensitive PII; and
- The PTA meets the requirements of conducting a PIA on simple systems containing routine information and limited use and access.

APPENDIX D

Summary of Management's Comments on the Recommendations

This table presents the management response to the recommendations in FHFA-OIG's report and the status of the recommendations as of the date of report issuance.

Rec. No.	*Corrective Action: Taken or Planned*	*Expected Completion Date*	*Monetary Benefits*	*Resolved:[a] Yes or No*	*Open or Closed[b]*
1.	FHFA will draft, disseminate, and implement a written Privacy Training and Implementation Approach Plan (Plan).	03/31/2012	$0	Yes	**Open**
2.	As part of the Plan, FHFA will identify those employees or offices that would benefit from additional job specific or role based privacy training based on increased responsibilities related to PII.	03/31/2012	$0	Yes	**Open**
3.	In conjunction with the described plan actions for recommendation 2, FHFA will develop and implement targeted role based training.	05/31/2012	$0	Yes	**Open**
4.	As part of the Plan, FHFA will develop and implement training for employees on when and why SORNs are required and how to draft them to meet Privacy Act requirements. FHFA's new employee training—which includes information regarding SORNS—will be updated to place greater emphasis on the requirements of the Privacy Act as it relates to systems of records. The new training will be incorporated into new employee and annual Privacy Awareness training during fiscal year 2012.	Fiscal Year 2012	$0	Yes	**Open**

Rec. No.	*Corrective Action: Taken or Planned*	*Expected Completion Date*	*Monetary Benefits*	*Resolved:[a] Yes or No*	*Open or Closed[b]*
5.	Currently, FHFA has a draft document, Procedure on How and When to Draft a Privacy Act System of Records Notice, which addresses when and why SORNs are required and how to draft one to meet Privacy Act requirements. The document will be posted on the FHFA Info Site and will form the basis for training employees on SORNs.	11/30/2011	$0	Yes	**Open**
6.	FHFA will update its *Privacy Threshold Analysis and Privacy Impact Assessment Guide* to address how routine database systems containing routine information with limited use and access are analyzed. Further, FHFA will update the PTA form to include a section that clearly identifies those systems that are "routine database systems." The form will require the individual completing the analysis to indicate an analysis was conducted and will include the following elements: the system was identified as a routine database system; the information collected is non-sensitive PII; and the PTA meets the requirements of conducting a PIA on simple systems containing routine information and limited use and access.	01/31/2012	$0	Yes	**Open**
7.	FHFA will draft agency-wide guidance on how and when privacy impact assessments will be	09/28/2012	$0	Yes	**Open**

Rec. No.	*Corrective Action: Taken or Planned*	*Expected Completion Date*	*Monetary Benefits*	*Resolved:*[a] *Yes or No*	*Open or Closed*[b]
	conducted for proposed rules of the Agency.				
8.	See response to recommendation 6 above.	01/31/2012	$0	Yes	**Open**
9.	FHFA's CPO will work with the CISO and system owners to draft and implement written policies and procedures for continuous monitoring of information systems with PII. FHFA—in coordination with all FHFA divisions and offices—will develop an agency-wide process for continuous monitoring of information systems containing PII.	09/28/2012	$0	Yes	**Open**

[a] Resolved means – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation; (2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation; or (3) Management agrees to the FHFA-OIG monetary benefits, a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the FHFA-OIG determines that the agreed-upon corrective actions have been completed and are responsive to the recommendations, the recommendations can be closed.

ADDITIONAL INFORMATION AND COPIES

For additional copies of this report:

- Call the Office of Inspector General (OIG) at: 202-408-2544
- Fax your request to: 202-445-2075
- Visit the OIG website at: www.fhfaoig.gov

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

- Call our Hotline at: 1-800-793-7724
- Fax us the complaint directly to: 202-445-2075
- E-mail us at: oighotline@fhfa.gov
- Write to us at: FHFA Office of Inspector General
  Attn: Office of Investigation – Hotline
  1625 Eye Street, NW
  Washington, DC 20006-4001