Privacy Impact Assessment Template

CLIENT MANAGEMENT SYSTEM (CMS)
(SYSTEM NAME)

This template is used when the Chief Privacy Officer determines that an IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
Senior Agency Official for Privacy
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024
(202) 649-3803
Privacy@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form ("IIF"; also referred to Personally Identifiable Information (PII)) is handled. PIAs are to be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates IIF from or about members of the public; or 2) initiates a new electronic collection of IIF for 10 or more members of the public. PIAs are not required for collections of information from Federal employees. IIF about government personnel generally is protected by the Privacy Act; however the Office of Management and Budget (OMB) encourages agencies to conduct PIAs on these Systems, as appropriate. System Owners and Developers are responsible for completing the PIA.

The guidance below has been provided to help System Owners and Developers complete a PIA.

Overview

- In this section, provide a thorough and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to consider include:
  - What is the purpose of the System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/Program's mission?
- This section fulfills the E-Government Act's requirement for an introduction for members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

FOR A PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- **Overview**
- **Section 1**
- **Section 2**
- **Section 6**

Section 1.0 Characterization of the Information

- Identify if the System contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.
- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider:
  - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or a private organization).
- If the System collects information from 10 or more members of the public, ensure that FHFA has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the Office of General Counsel for assistance.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports FHFA's or the Office's/Division's/Program's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).
- The retention periods for data/records that FHFA manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.
- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

Section 4.0 Notice, Access, Redress and Correction

- The Privacy Act requires that "each agency that maintains a System of records shall maintain in its records 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 by executive order of the President." 5 U.S.C. 552a(e)(1).
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the System retrieves information by an individual's name or other unique identifier (e.g. social security number) it is a Privacy Act System and may need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact the Chief Privacy Officer.
- If a name or other unique identifier is not used to retrieve information, it is possible that the System is not a Privacy Act System. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.
- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors, if appropriate.
- Any employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.

Section 5.0 Sharing and Disclosure

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the Systems/applications. As an example, if your System/application shares data with another System/application, ask yourself whether you have access to the data in the interfaced System/application. If so, then your answer is yes and an explanation is needed.
- Also consider "other" users who may not be obvious as those listed, such as the General Counsel Accountability Office or the FHFA Office of Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN

under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.

- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

Section 6.0 Access and Security

- Access to data by a user (i.e. employee or contractor personnel) within FHFA is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.
- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.
- The System owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open Systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the System and/or application. However, restrict access when users do not need to have access to all the data.
- When a contract provides for the operation of a System on behalf of FHFA, the Privacy Act requirements must be applied to such a System. Contact the Contracting Officer or Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The Certificate and Accreditation (C&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are System-based means by which the ability to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The C&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- According to OMB Circulars A-123 and A-130, every System/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data. For instance, in computerized Systems the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the System and is transparent to the user. Describe these processes in response to this question.
- All employees, including contractors, have requirements for protecting information in Privacy Act Systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

PIA FORM

Overview

This section provides an overview of the System and addresses the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

Date submitted for review: August 23, 2013

System Name: Client Management System (CMS)			
System Owner(s):			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Owen Highfill (Conservatorship Operations Specialist)	Owen.highfill@fhfa.gov	Office of Conservatorship Operations	202-649-3042
Mary Johnson (Manager, Conservatorship Operations)	Mary.Johnson@fhfa.gov	Office of Conservatorship Operations	202-649-3043
System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to the agency's mission.			
The Client Management System (CMS) is FHFA's primary consumer communications tracking software. CMS tracks consumer communications to meet FHFA's mission as regulator and conservator of Fannie Mac and Freddie Mac and regulator of the FHL Banks. CMS is used to collect basic information (data fields) from individuals or their representative who contact FHFA with an inquiry, comment, or question. The information collected is stored in the CMS system to allow for tracking consumer inquiries and response times. The CMS system includes links to IMS folders that contain complaint/inquiry level supporting documents.			

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the System?	Information is collected on the individual who submits a complaint or inquiry, or his/her representative (if applicable), and the issue or question.
1.2	What are the sources of the information in the System?	Information is provided by the individual and/or his/her representative. In addition, information may have been sent to a separate party (e.g., state or federal government agency or office) that in turn has forwarded it to FHFA. Information related to the processing and disposition of the complaint/inquiry is provided by FHFA and FHFA regulated personnel, if applicable.
1.3	Why is the information being collected, used, disseminated, or maintained?	Information is collected to inform FHFA and FHFA regulated entities of consumer issues or questions, to allow for a response to be generated for the consumer, analysis of industry issues or emerging topics, and to identify specific risks and/or potential issues at the FHFA regulated entities that may require closer review by FHFA Examination and Supervision personnel.
1.4	How is the information collected?	Per directions provided on FHFA's external website, the consumer submits information via telephone, email, fax and/or letter. Information from that communication is entered in CMS database.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Since FHFA does not require PII data from individuals and in fact encourages them to not submit this type of information, risks to an individual's privacy are low. However, there are instances in which an individual may voluntarily choose to send PII data to FHFA. In this instance, FHFA takes two steps to ensure that the risks to an individual's privacy remain low: (1) access to the CMS system is limited to those in OCO and DER who need to know; and (2) access to the IMS file folders with supporting documents is restricted to those in OCO and DER who need to know.

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	Describe the uses of information.	Information is used to inform internal FHFA personnel, FHFA regulated entities and/or FHFA OIG personnel about trending consumer issues. Upon receipt, those parties may choose to review, investigate and resolve the issue. In addition, information is used to inform the appropriate person/s at the FHFA regulated entity. Upon receipt, those parties will review, investigate, resolve the issue, and contact the complainant/inquirer as appropriate.
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	Access to the CMS system (and linked files) is limited to those individuals within OCO and DER who work directly with the consumer and/or review the consumer complaints process at the Enterprises. In addition, information is forwarded only to those individuals within FHFA, the FHFA-regulated entities or FHFA OIG who work with consumers or who have a need to know.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is information retained?	Information is retained for seven years.
3.2	Has a retention schedule been approved by FHFA's Records Management Officer and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes. The Records Management Office (RMO) has reviewed and established a retention schedule for consumer-related information. See FHFA Comprehensive Records Retention Schedule, Revised Version – 07/26/2012, N1-543-11-1 Item 1.5, Consumer Communications Records.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risk are low since FHFA only retains the information for seven years and the information is stored in a secure environment, with limited access.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	Yes. Federal Register/Vol. 74, No. 127 / Monday, July 6, 2009 / Notices, FEDERAL HOUSING FINANCE AGENCY [No.2009-N-08], Privacy Act of 1974; System of Records, pages 31953-31954, FHFA-3, "Correspondence Tracking System."
4.2	Was notice provided to the individual prior to collection of information?	Yes. Notice is provided on the FHFA website at http://www.fhfa.gov/default.aspx?Page=369
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes. However, not providing the information limits the ability of personnel at FHFA and/or the FHFA regulated entity to review, analyze, resolve and respond to the consumer's issue.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may gain access to their information by following the procedures set forth in the Correspondence Tracking System SORN (FHFA-3).
4.5	What are the procedures for correcting inaccurate or erroneous information?	Individuals may request that their records be corrected following the procedures set forth in the Correspondence Tracking System SORN (FHFA-3_.If inaccurate or erroneous information is identified, CMS data fields are updated and/or parties who received the inaccurate or erroneous information are notified of the errors and provided with corrections.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	Depending on the issue, the information may be shared with FHFA personnel in various offices; e.g., General Counsel, Examination and Supervision, and/or Housing, Mission and Goals. Generally, information is shared for the purpose of informing them (as an FYI) of a complaint or issue. Upon receipt, the party receiving it will decide what action, if any, is appropriate and will be taken. Generally, OCO personnel do not disclose PII-related information to internal parties. However, OCO cannot control the consumer's inclusion of PII in documents he/she chooses to provide to FHFA – other than through strong dissuasion. Internal parties may need access to documents provided by the consumer in order to review and assess the situation.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	Depending on the issue, the information may be shared with an FHFA regulated entity and/or the FHFA-OIG. OCO also forwards complaints that do not fit within FHFA's purview to the US Department of Housing and Urban Development (HUD) when appropriate. The purpose of sharing is to inform the recipient, and to allow the recipient to review, analyze and take action, if appropriate. Generally, OCO personnel do not disclose PII-related information to external parties. OCAC-CC generally limits the information to disclosing the complainant's name and the related property address. However, OCAC-CC cannot control the consumer's inclusion of PII in documents he/she chooses to provide to FHFA – other than through strong dissuasion. External parties may need the consumer's documents in order to review, assess and resolve the situation.
5.3	Is the sharing of PII outside the agency compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	Generally, PII is not collected or shared but when it is it is limited to only that which is sufficient to allow for an understanding of the complaint/inquiry and to initiate action, if appropriate. Typically, the information that is shared is the complainant's (and/or borrower's) name and mortgaged or REO property address.

#	Question	Response
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Generally, PII-related information that FHFA provides is the same information the FHFA-regulated entity has on its system or has ready access to via the lender or servicer. Therefore, the risks arise from the transmission of the information rather than the information itself. FHFA limits its transmission to specific individuals or units at FHFA-OIG , the FHFA regulated entities, and HUD. External sources, including the FHFA-OIG, the Enterprises, and HUD, send electronic receipts back to FHFA acknowledging that they have received the complaints.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? If so, attach a copy to this PIA.	Users with direct access to the system are OCO and DER personnel specifically assigned to consumer communication. It is estimated that the number of persons will range from 4 – 6. A CMS user guide is under development and will address access. The Consumer Communications Policy and Procedures have been updated and are currently undergoing the red folder review and approval process.
6.2	Will non-FHFA personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will the agency control their access and use of information? Are there procedures documented in writing? If so, attach a copy to this PIA.	Non-FHFA personnel do not have direct access to the system.
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	OTIM will and has provided general training of FootPrints and the CMS. One-on-one training will be provided to OCO users by the System Administrator. In addition, a CMS sser guide will be provided once developed.

#	Question	Response
6.4	What technical safeguards are in place to protect the data?	OTIM is responsible for establishing and maintaining technical safeguards. Each user must log in using a unique user ID and password. The application data will be stored in an MS SQLServer database located on a secure server. Employees can only access the data through the application as ad-hoc access to the data is prohibited unless approved by the system owner. System and Database administrators will be granted privileges sufficient to successfully complete required tasks.
6.5	What auditing measures are in place to protect the data?	A tracking log exists to track user entries and changes to data fields
6.6	Has a C&A been completed for the System or Systems supporting the program? If so, provide the date the last C&A was completed. If not, and one is required, provided the expected completion date of the C&A.	OTIM is responsible for completion of the C&A. The C&A for Footprints is in progress and is expected to be completed by 9/15/2013.

Signatures

Owen Highfill System Owner (Printed Name)	Owen Highfill System Owner (Signature)	9/10/13 Date
Mary Johnson System Owner (Printed Name)	Mary D. Johnson System Owner (Signature)	9/10/2013 Date
Jude Corina System Developer (Printed Name)	J. Corina System Developer (Signature)	9/11/2013 Date
Ralph Mosios Chief Information Security Officer (Printed Name)	Ralph Mosios Chief Information Security Officer (Signature)	10/29/2013 Date
R. Kevin Winkler Chief Information Officer (Printed Name)	 Chief Information Officer (Signature)	10/15/13 Date
David A. Lee Chief Privacy Officer (Printed Name)	 Chief Privacy Officer (Signature)	11/19/2013 Date