Privacy Impact Assessment Template

FHFA.GOV
(SYSTEM NAME)

11/6/2018
DATE

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

Complete this template and forward to the Senior Agency Official for Privacy.

David A. Lee
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 Personally Identifiable Information (PII) is collected, stored, maintained, and shared. A PIA must be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates PII from or about members of the public; or 2) initiates a new electronic collection of PII for 10 or more members of the public. System Owners are primarily responsible for completing the PIA with assistance from IT developers, IT security officers, and the Privacy Office.

OVERVIEW SECTION

- Provide a thorough, complete, 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 to 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.

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 will 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 FHFA's Privacy Office.
- 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 GAO, or FHFA's 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 greater access – i.e. 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 Security Assessment and Authorization (SA&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 SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- 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.
- 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: 11/5/2018

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Amy Lakroune	Amy.Lakroune@FHFA.gov	OCAC	(202) 649.3031

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.

"FHFA.gov Online Forms" are owned by OCAC.

Individuals who contact FHFA with questions, comments, to file a complaint or appeal, to request or provide information, to request consumer assistance, to respond to a proposed rule, or who wish to conduct business with FHFA.

FHFA Online Forms contain information submitted by individuals or their representatives, to FHFA. FHFA will use this information to communicate with and respond to individuals who submit a form online with FHFA.

The system contains the following information about individuals who submit a form on FHFA's Web site:
Name, address, telephone number, fax number, email address, property information, borrower information, organization name and type, government agency name and type, job position, and representative of submitter; correspondence and records of communication between FHFA and individuals submitting information, including copies of supporting documents; information regarding a company wishing to do business with FHFA (*i.e.*, company name, address, telephone number, Web site address, description of supplies or services offered, years of experience, DUNS, GSA, NAICS and GWAC number, organization affiliations, special category status, and past performance references), and related information.

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 being collected, used, disseminated, or maintained in the System?	Records contain the following: Contact information for individual submitters,(information about an individual who submits a form on FHFA's Web site: Name, address, telephone number, fax number, email address, property information, borrower information, organization name and type, government agency name and type, job position, and representative of submitter; correspondence and records of communication between FHFA and individuals submitting information, including copies of supporting documents; information regarding a company wishing to do business with FHFA (*i.e.*, company name, address, telephone number, Web site address, description of supplies or services offered, years of experience, DUNS, GSA, NAICS and GWAC number, organization affiliations, special category status, and past performance references), and related information.
1.2	What or who are the sources of the information in the System?	Individuals who contact FHFA with questions, comments, to file a complaint or appeal, to request or provide information, to request consumer assistance, to respond to a proposed rule, or who wish to conduct business with FHFA.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	FHFA uses the records in this system to communicate with individuals who submit a form online with FHFA. The forms will allow FHFA to respond to complaints, appeals, inquires and requests for information; to review and post comments on proposed rules/ regulations; to review feedback received on FHFA proposed or implemented initiatives; and to compile a list of potential vendors and contractors. The forms will also assist FHFA and those who will respond to the submitter with consumer issues involving Fannie Mae, Freddie Mac, and the Federal Home Loan Banks.
1.4	How is the information provided to FHFA?	Information is input by individuals on FHFA.gov via the online forms available at: https://www.fhfa.gov/AboutUs/Contact.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss, or compromise of the information will/can affect an individual's privacy.	Risk of loss; identity theft; data integrity.

#	Question	Response
1.6	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit and in storage.	Social security numbers are not being collected.

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	How will the information be used and for what purpose?	FHFA uses the records in this system to communicate with individuals who submit a form online with FHFA. The forms will allow FHFA to respond to complaints, appeals, inquires and requests for information; to review and post comments on proposed rules/ regulations; to review feedback received on FHFA proposed or implemented initiatives; and to compile a list of potential vendors and contractors. The forms will also assist FHFA and those who will respond to the submitter with consumer issues involving Fannie Mae, Freddie Mac, and the Federal Home Loan Banks.
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.	Records are maintained in electronic format and stored in a computerized database. Computerized records are safeguarded through use of access codes and other information technology security measures. Paper records are safeguarded by locked file rooms, locked file cabinets, or locked safes. Access to the records is restricted to those who require the records in the performance of official duties related to the purposes for which the system is maintained.

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 the information retained?	Content submitted via FHFA Online Forms is owned by business unit offices – so retention schedules vary.

#	Question	Response
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	(General) web content retention is addressed in OCAC's 2018 File Plan (5.5b – web content). Records considered temporary – destroy or delete three (3) years after cutoff. OCAC owns the FHFA.gov Online Forms system/structure, however, content within the topical databases is owned by respective business units and acted upon, captured and/or retained per respective office/division file plans.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Risk of loss; identity theft; data integrity; misuse or inadvertent disclosure.

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.	**SORN: FHFA -22 Online Forms (published in Federal Register 11/6/2013)** https://www.fhfa.gov/SupervisionRegulation/Rules/Pages/Privacy-Act-of-1974;-System-of-Records-Notice-of-proposed-revision-of-an-existing-system-of-records-and-establishment-of-a-.aspx
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Yes, every form on FHFA.gov has the following privacy notice: Privacy Act Notice* This notice is provided pursuant to the Privacy Act of 1974 (Privacy Act), as amended, 5 U.S.C. § 552a. The collection of information is to process and/or respond to your complaint, appeal, inquiry, request for information, to review and post comments on proposed rules/regulations, to review feedback received on FHFA proposed or implemented initiatives, and to compile a list of potential vendors and contractors. The records are used in accordance with Systems of Records Notices (SORN), FHFA-3 Correspondence Tracking System, FHFA-20 Telecommunications System, and FHFA-22 Online Forms. You can view these SORNs by clicking **here** and **here** and **here**. Although providing this information is voluntary, failure to provide the requested information may result in your complaint, appeal, inquiry, request, comment, or feedback not being processed and may make it more difficult for FHFA to respond to you.

#	Question	Response
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	Per the Privacy Act Notice, individuals are informed that "although providing this information is voluntary, failure to provide the requested information may result in your complaint, appeal, inquiry, request, comment, or feedback not being processed and may make it more difficult for FHFA to respond to you."
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals can direct requests for access to the Privacy Act Appeals Officer in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Individuals can direct requests to contest or appeal an adverse decision for a record to the Privacy Act Appeals Officer in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204.

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?	Access varies by form and on a case-by-case basis. "Homeowner Assistance" requests are handled by OCAC Consumer Assistance team and may be shared with Ombudsman, and/or appropriate business office; "Data and Research" requests are directed to specific offices that handle particular regulated entities and or research; "Doing Business with Us" is managed by OMWI, and may be shared with OBFM, Contracting Office and OGC; "General Questions or Comments" will be shared with appropriate business offices; "Input on Topic" shared with respective business office(s) depending on the topic (case-by-case), "Mortgage Translations" assistance is shared by team leads with appropriate team/offices who might best address requests/inquiries.
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.	***Some (form) submissions are posted to publicly viewable areas of FHFA.gov immediately without redaction.*** Those not specifically public, depending on the subject matter, may be shared with regulated entities (Fannie Mae, Freddie Mac, or Federal Home Loan Banks), FHFA OIG, HUD, Treasury, or other regulatory agencies, or members of Congress as appropriate or others per SORN 22.

#	Question	Response
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.	Yes. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained herein may specifically be disclosed outside FHFA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: (1) When (a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (b) FHFA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by FHFA or another agency or entity) that rely upon the compromised information; and (c) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with FHFA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. (2) Where there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local, tribal, foreign or a financial regulatory organization charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing a statute, or rule, regulation or order issued pursuant thereto. (3) To any individual during the course of any inquiry or investigation conducted by FHFA, or in connection with civil litigation, if FHFA has reason to believe that the individual to whom the record is disclosed may have further information about the matters related therein, and those matters appeared to be relevant at the time to the subject matter of the inquiry. (4) To any individual with whom FHFA contracts to reproduce, by typing, photocopy or other means, any record within this system for use by FHFA and its employees in connection with their official duties or to any individual who is utilized by FHFA to perform clerical or stenographic functions relating to the official business of FHFA. (5) To members of advisory committees that are created by FHFA or by Congress to render advice and recommendations to FHFA or to Congress, to be used solely in connection with their official, designated functions and is related to the purpose for which FHFA collected the records. (6) To a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. (7) To contractor personnel, grantees, volunteers, interns, and others performing or working on a contract, service, grant, cooperative agreement, or project for FHFA.

#	Question	Response
		(8) To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings, or in response to a subpoena from a court of competent jurisdiction. (9) To the Office of Management and Budget, Department of Justice (DOJ), Department of Labor, Office of Personnel Management, Equal Employment Opportunity Commission, Office of Special Counsel, Department of Homeland Security, or other Federal agencies to obtain advice regarding statutory, regulatory, policy, and other requirements related to the purpose for which FHFA collected the records. (10) To DOJ, (including United States Attorney Offices), or other Federal agency conducting litigation or in proceedings before any court, or adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: 1. FHFA; 2. Any employee of FHFA in his/her official capacity; 3. Any employee of FHFA in his/her individual capacity where DOJ or FHFA has agreed to represent the employee; or 4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and FHFA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which FHFA collected the records. (11) To the National Archives and Records Administration (NARA) or other Federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906. (12) To a Federal agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function. (13) To Fannie Mae, Freddie Mac, or the Federal Home Loan Banks as it relates to the purpose for which FHFA collected the record.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	Possibility of loss of control, risk of loss; identity theft; data integrity; misuse or inadvertent disclosure are mitigated by FHFA network security protocols.

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?	FHFA.gov and FHFA Intranet Posting and Maintenance Procedures

#	Question	Response
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?	Yes, on occasion contractor personnel will need to access information, to export/share with owner offices or to correct and/or approve submissions prior to publication on FHFA.gov website. Access is provided to individuals selected by owner offices upon request from appropriate managers and/or content owners. User access, for contractor and FHFA staff, is controlled through internal control access procedures. Best practices follow the principle of "least privilege." Users are given the lowest permission levels they need to perform their assigned tasks.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System?	When new forms are added to FHFA.gov (or new topics, under Request for Information form), respective topic owner/users are given access to submissions and are notified by the system when comments/input are submitted via FHFA.gov. Individuals are trained by OCAC to access, review and approve input when needed. (Sample instruction/training submitted separately).
6.4	Describe the technical and administrative safeguards in place to protect the data?	Data submitted in online forms is stored in a SharePoint database, accessible only to authorized members of OCAC. Access is restricted using SharePoint access control groups, administered by the FHFA.Gov system owner.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	The FHFA.Gov SharePoint environment is configured to audit all allowable events, including editing content types, opening documents, viewing items in lists, etc. Weekly audit reports of these events are delivered to the FHFA.Gov system owner who reviews them for unusual activity.
6.6	Has a SA&A been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	Yes. The last FHFA.Gov SA&A was completed on September 11, 2018.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued. If not, when do you anticipate such ATO being issued?	The latest ATO was signed on September 12, 2018 as part of the Ongoing Authorization of FHFA Information Systems.