



Privacy Impact Assessment Template

ADVISORY COMMITTEE MANAGER
(SYSTEM NAME)

DECEMBER 6, 2022
DATE

Privacy Officer
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024
(202) 649-3091
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 that 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

Provide an overview of the System and address 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.

System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Samuel Frumkin	Samuel.Frumkin@fhfa.gov	Office of the Director	202-649-3108
<p>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.</p>			
<p>Pursuant to the Federal Advisory Committee Act of 1972 (PL 92-463, 5 USC App 1) (FACA), FHFA will form and use federal advisory committees to obtain objective advice and recommendations regarding agency programs and policies. FHFA will collect information directly from individuals who apply for membership on an advisory committee. The information collected may include contact information, resumes, work experience, and affiliations. The agency may also collect U.S. citizenship status. The system will be used by the reviewing panel to determine eligibility and select applicants to fill vacant positions on FHFA advisory committees.</p> <p>Members who will serve as Special Government Employees will be required to file a financial disclosure form prior to appointment on the committee. The forms are stored in FD Online, which is a FedRAMP authorized system hosted by Intelliworx. Such financial information will not be collected by or shared with this system.</p>			

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?	Application materials including but not limited to resumes, cover letters, affiliations, disclosing applicants' names, business and personal email addresses, business and personal mailing addresses, professional employment history, and professional associations and affiliations. Financial information may be considered in addressing a potential conflict for Special Government Employees who seek membership

#	Question	Response
		on a committee. This information, however, will not be collected or otherwise used by this information system.
1.2	What or who are the sources of the information in the System?	Individuals applying for membership on an FHFA advisory committee.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information will be used to determine eligibility and select applicants to fill vacant positions on advisory committee(s).
1.4	How is the information provided to FHFA?	Directly from individuals who are interested in FHFA advisory committee membership.
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.	The risk to an individual’s privacy if the data is lost or compromised is identify theft, loss of future employment opportunities, embarrassment, and/or misuse of the individual’s personal information.
1.6	Are Social Security numbers are being collected or used in the system?	No
1.7	If SSNs are collected or used in the system, 1) describe in detail the business justification for collecting or using SSNs; 2) the consequences if SSNs are not collected or used, and 3) how the SSNs will be protected while in use, in transit and in storage.	N/A

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?	The system will be used for storing and reviewing application materials.
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 will be limited to only those employees that are permitted to perform the Advisory Committee Manager selection and review functions.

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?	<p>Substantive Committee Records (Non-Grant Review Committees) and Substantive Audiovisual Records (Non-Grant Review Committees) are permanent records, while Grant Review Committee Records, Committee Accountability Records, Non-substantive Committee Records, and Committee Management Records are temporary records. Substantive Committee Records (Non-grant Review Committees) are transferred to the National Archives and Records Administration (NARA) when records are 15 years old or upon termination of a committee, whichever is sooner. Substantive Audiovisual Records (Non-grant Review Committees) are transferred to the NARA when records are three years old or upon termination of a committee, whichever is sooner. Grant Review Committee Records are destroyed upon termination of a committee. Committee Accountability Records are destroyed when six years old, except when longer retention is required for business use. Non-substantive Committee Records are destroyed when superseded, obsolete, no longer needed, or upon termination of the committee, whichever is sooner. Committee Management Records are destroyed when three years old, three years after submission of a report, or three years after superseded or obsolete, as appropriate; longer retention is authorized if required for business use.</p>
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.	Records will be managed in accordance with FHFA’s Comprehensive Records Schedule (CRS) Item 6.2.01-06, as applicable.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are minimal risks associated with the length of time the data is retained in this System. Access to this System and the information therein is limited to certain FHFA employees who have been granted access to this System by the System Owner.

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.	FHFA 30, Advisory Committee Manager is expected to be published by the end of calendar year 2022.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	A Privacy Act Statement is being drafted and will be included in the notice presented to members of the public when applying for advisory committee membership.
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?	Applicants are not required to serve on an advisory committee. An applicant’s submission of their application materials is voluntary. If applicants forgo submitting the required information, they will not be considered for appointment to a FHFA advisory committee.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may submit a Privacy Act request to FHFA’s Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Instructions for submitting Privacy Act requests are available on FHFA’s website Privacy Page, located at https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx .
4.5	What are the procedures for correcting inaccurate or erroneous information?	Applicants may send an email to the Advisory Committee Manager’s dedicated email address to request changes to their information or provide additional details or updates. Individuals may also submit a Privacy Act request to FHFA’s Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Instructions for submitting Privacy Act requests are available on FHFA’s website Privacy Page, located at https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx

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?	Information is shared with the reviewing panel, consisting of FHFA division heads, and accordingly that information may be shared with any FHFA division or office, as needed for the committee membership selection process.
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.	The names of individuals selected for membership on a committee will be shared with the general public via committee meetings, as required by FACA and the Sunshine Act (PL 94-409, 5 USC 552b). The names, zip codes, and employment information of Committee members will be provided to the FACA Database at the General Services Administration (GSA), as required by FACA. Subject to above and the applicability of routine uses described below in response to Question 5.3, information collected by this system is intended only for use by FHFA and is not intended to be shared with third party organizations, federal agencies, or the general public.
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.	<p>In addition to the general public, information from this System may be shared to external entities in accordance with the following routine uses:</p> <p>(1) To appropriate agencies, entities, and persons when—(a) FHFA suspects or has confirmed that there has been a breach of the system of records; (b) FHFA has determined that as a result of a suspected or confirmed breach there is a risk of harm to individuals, FHFA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons as reasonably necessary to assist with FHFA’s efforts to (i) respond to a suspected or confirmed breach or (ii) prevent, minimize, or remedy harm caused by such breach.</p> <p>(2) To a federal agency or federal entity, when FHFA determines information from this system of records is reasonably necessary to assist the recipient agency or entity in: (a) responding to a suspected or confirmed breach; or (b) preventing,</p>

#	Question	Response
		<p>minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or to national security, resulting from a suspected or confirmed breach.</p> <p>(3) When 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 (<i>e.g.</i>, 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, rule, regulation or order issued pursuant thereto.</p> <p>(4) 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 the individual to whom the record is disclosed may have further information about the matters related thereto, and those matters appeared to be relevant and necessary at the time to the subject matter of the inquiry.</p>
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	The risk to an individual's privacy if the data is lost or compromised is identity theft, loss of future employment opportunities, embarrassment, or misuse of the individual's personal information. These risks are mitigated by limiting any external sharing to that which is required by law.

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? <u>If so, attach a copy to this PIA.</u>	Procedures will be drafted once roles and responsibilities have been identified by the relevant offices. Notwithstanding, only those with an official business need will be granted access to this information system.
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? <u>If so, attach a copy to this PIA.</u>	No.
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?	All FHFA employees are required to undergo security, privacy, and Records and Information Management (RIM) training for use of FHFA systems at onboarding and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII.
6.4	Describe the technical/administrative safeguards in place to protect the data?	Data will be stored on the FHFA General Support System (GSS) and protected by the safeguards described in the FHFA GSS PIA.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Data will be stored on the FHFA GSS and covered by GSS auditing capabilities that include logging of file access and modification that are available to information owners to review as needed.
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.	The FHFA GSS is in the ongoing authorization phase of the Risk Management Framework and undergoes annual control assessments.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? If not, when do you anticipate such ATO being issued?	The most recent ATO for the FHFA GSS was issued on September 29, 2022.