Privacy Impact Assessment Template

FHFA IDEALSCALE
(SYSTEM NAME)

September 21, 2022
(DATE)

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@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 Information Technology (IT) system or project that collects, maintains, or disseminates PII that can be used to identify a specific individual; or 2) initiates a new electronic collection of PII for 10 or more members of the public, which includes any information in an identifiable form permitting the physical or online contacting of a specific individual.

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

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 or Mobile Phone Number**
Donald McLellan	Donald.Mclellan@FHFA.gov	OCOO	202-649-3036

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 FHFA IDEASCALE employee engagement/innovation platform is a fully integrated digital platform and site ("Site") for increased employee engagement and innovation activities such as crowdsourcing, idea sharing, and agency-wide discussion. This platform will be used to regularly monitor the pulse of the workforce to continuously gain employees' views regarding products/services, communications, relationships, and overall work environment.

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?	Employee names, email addresses, office affiliations, usernames and passwords, zip codes, and phone numbers. Additionally, any ideas submitted by an employee or during a host group discussion on process improvement/service and product innovation, which could include PII that does not qualify as "sensitive PII," will be collected. Sensitive PII is defined in the Terms of Use for this System to include, but not be limited to, "any information about yourself or another person that may relate to health or medical conditions, social security numbers or national identifiers, credit card, bank account or other financial information, other information concerning trade union membership, sex life, political

		opinions, criminal charges or convictions, religious or philosophical beliefs, racial or ethnic origin, or other sensitive matters."
1.2	What or who are the sources of the information in the System?	Employee names, email addresses, office affiliations, zip codes, and phone numbers are obtained from the Active Directory. Information, suggestions, requests, and other submissions are provided by employees through the System. Passwords and usernames come directly from the submitting employee. There may be occasions when the Site is used to invite comments or suggestions from the public or selected stakeholders. Members of the public responding to this invitation will submit their suggestions or comments via a "non-employee" log-in portal. In such instances, the names and email addresses of the submitting non-employee or stakeholder will be retained in addition to the suggestion or comment submitted.

#	Question	Response
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The FHFA IDEASCALE employee engagement/innovation platform and site is a fully integrated digital platform for increased employee engagement and innovation activities such as crowdsourcing, idea sharing, and agency-wide discussion. This platform will be used to regularly monitor the pulse of the workforce to continuously gain employees' views regarding products/services, communications, relationships, and overall work environment.
1.4	How is the information provided to FHFA?	Employee names, email addresses, office affiliations, zip codes, and phone numbers are retrieved from the Active Directory through interface with this System. Information, suggestions, requests, and other submissions are provided directly by employees through the employee portal. For future instances where submissions may be sought from the public, members of the public will offer their suggestions, requests, and other submissions through a non-employee portal available at FHFA.gov.
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 privacy is low because the PII data elements of FHFA employees collected from the Active Directory are already publicly available. The risk to an individual's privacy if the data is lost or compromised consist of identity 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. Terms of Use that expressly prohibit the submission of Social Security Numbers are presented to each employee upon first accessing this System. Each employee must abide by and acknowledge these terms in writing in order to access the System.
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?	This System will use the information collected to increase employee engagement and service/product innovation.

#	Question	Response
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.	Employees are required to review, abide by, and acknowledge by signature the Terms of Use for the System. The Terms of Use prohibit the submission of any "sensitive" personally identifiable information to the Site, which may include, but not be limited to, information about the person or another person that may relate to health or medical conditions; social security numbers or national identifiers; credit card, bank account or other financial information; information concerning trade union membership; sexual orientation; political opinions; criminal charges or convictions; religious or philosophical beliefs; racial or ethnic origin; or, other sensitive matters. Before publication on the Site, all submissions are reviewed by a Site Moderator for compliance with the Terms of Use. The Terms of Use are presented and required to be accepted by employees at their first instance of logging onto the Site and are also available on each campaign landing page of the Site. Other appropriate safeguards, as described below in Section 6, have also been applied.

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?	Because this System interfaces with the Active Directory to obtain employment-related information for FHFA employees, information pulled from the Active Directory will remain unless/until employment with FHFA is terminated. Submissions by employees, for campaigns and other uses set forth in the Terms of Use, that are rejected or no longer subject to consideration for a campaign or as otherwise described in the Terms of Use are retained for seven years. Upon the

		expiration of this seven-year period, those records will be reviewed by the System Owner to evaluate any possible need for continued retention of such documents. If the System Owner determines the files are no longer needed, they will then be subject to deletion.
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.	*FHFA Comprehensive Records Schedule (CRS)* Item 6.1b— includes records not covered elsewhere in this schedule that are related to projects with department-wide or administrative impact, including but not limited to, correspondence, memoranda, reports, studies and meeting minutes.
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 FHFA employees.

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. FHFA-7 - Mail, Contacts, Telephone, and Other Lists applies to this System.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Prior to accessing the Site, users will be provided a Privacy Act Statement and the Site's Terms of Use.
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?	Employee names, email addresses, office affiliations, zip codes, and phone numbers are directly obtained by this System from the Active Directory and therefore employees do not have the opportunity to decline to provide this information. Submissions of ideas, comments, requests, or questions to or through this System are on a voluntary basis. The consequence of not submitting ideas, comments, requests, or questions is that the employee's ideas, comments, requests, or questions regarding a campaign posted to the Site

		will not be provided to FHFA for consideration.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	All employees will have access to the Site and their information at all times their FHFA issued computer or cell phone, or accessing FHFA's network as permitted. Individuals may also submit a Privacy Act request to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(b) to gain access to information included in the Site.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Site moderators will review all submitted ideas before general posting on the platform to ensure they do not violate the Terms of Use. Individuals may submit a Privacy Act Request to the FHFA Privacy Office to correct or amend information contained on the Site using the instructions provided on FHFA's 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?	The System Owner for this Site is employed within the Office of the Chief Operating Officer (OCOO). However, this is an open engagement platform for all employees. All postings will be available to all employees. Information posted on the internal portal will not be shared outside of the Agency or with non-FHFA personnel.
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.	On special occasion, certain documents will be shared with selected stakeholders for comments. A separate access portal will be set up for such instances. Non-FHFA employees will not have access to the internal FHFA IDEASCALE employee portal. In addition to the above and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records or information contained in this System 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, foreign or a financial self-regulatory organization charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto; (3) In the discretion of FHFA, 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; and (4) In the discretion of FHFA, 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.

5.3	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, any sharing of PII outside of FHFA is compatible with the original information collection and is covered by any one or more of Routine Uses (1) through (4) identified in response to Question 5.2, above.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	On the rare occasion in which FHFA might use this Site to solicit public comments on specific documents, the privacy risk would be minimal because the System will only collect names and/or email addresses.

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?	The Site is restricted to FHFA employees who are currently listed in the Agency's Office of Human Resources Management (OHRM) employee Active Directory database. Once access to the Site is granted, employees must abide by the Terms of Use, which they are required to acknowledge in writing, to maintain access.
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?	During development and testing of this System, vendor employees have access to the System and information therein solely to provide training to FHFA employees. Once the System is put into production, no non-FHFA employees will have or be granted access to the System or information therein, except for vendor employees or contractors upon request and only for technical support. All vendor employees and contractors are required to sign a non-disclosure agreement and are subject to a criminal background investigation. All PII collected by this System is only used to provide the contracted services to its customers and their users while those accounts are active. Upon closure of a user's account, any PII previously collected will only be used to address the System's legal obligations, as applicable.
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?	Initial, one-time, training will be provided to all employees via live presentations. Pre-recorded trainings will be posted on the Agency's learning platform, FEDtalent. All FHFA employees are required to undergo security, privacy, and RIM training for use of FHFA systems at onboarding and annually thereafter.
6.4	Describe the technical/administrative safeguards in place to protect the data?	IdeaScale is authorized under the Federal Risk and Authorization Management Program (FedRAMP). FHFA has developed Customer Controls that describe FHFA's implementation of controls for which the Agency is responsible. Such controls include procedures for securely managing access to the System, assigning roles based on the concept of least privilege, reviewing audit logs, and securing configuring the system.

6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	The System captures logs of all user authentication attempts and all application events. At least quarterly, the System Owner will review the audit log reports and notify the Office of Technology and Information Management (OTIM) if any unusual activity was observed.
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.	IdeaScale received its initial FedRAMP Authorization on October 19, 2017. It is in the continuous monitoring phase of the FedRAMP program and FHFA reviews the status of ongoing assessments at least annually.
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?	FHFA plans to issue an Agency Authorization to Use (ATU) for IdeaScale in September 2022.