Privacy Impact Assessment Template

FINANCIAL TECHNOLOGY (FINTECH)
(SYSTEM NAME)

DECEMBER 5, 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 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 Phone Number**
Liang Jensen	Liang.Jensen@fhfa.gov	DCOR/OGSI, OFT	(202) 649-3464

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.

Fintech and the FHFA office supporting this information system (the Fintech Office) serve as a strategic principal point-of-contact and a centralized information clearing house to support FHFA in making informed decisions, addressing emerging risks, and advancing mission priorities as they relate to housing finance fintech and innovations. Fintech incorporates the principle of "responsible innovation" into its activities, balancing the value of new ideas, products, and operational approaches with the need for effective risk management and corporate governance. Responsible innovation includes consideration and mitigation of possible adverse effects of innovation on housing finance system stability, equitable access of consumers to affordable and sustainable mortgage credit, and the competitive environment of the primary or secondary mortgage markets.

Fintech engages with market participants, industry, non-profits, consumer groups, and academia to facilitate the sharing of best practices of housing finance fintech and innovations. As part of the engagement process, FHFA will in certain instances collect information from individuals and/or companies who seek information or seek to participate in activities or initiatives hosted by Fintech. This includes, but is not limited to, listening sessions, forums, office hours, and tech sprints. FHFA may also review information to ensure that prospective participants do not have conflicts or issues that may disqualify them from working with FHFA.

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?	Fintech records include general contact and employment information for individuals and/or companies who seek information or seek to participate in activities or initiatives hosted by the Fintech Office. Fintech records also include information supporting innovation ideas and recommendations provided by market participants, industry, non-profits, consumer groups, and academia, as well as recordings or other records of listening sessions, forums, office hours, and tech sprints.
1.2	What or who are the sources of the information in the System?	Individual members of the public and/or companies who seek information or seek to participate in activities or initiatives hosted by the Fintech Office.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The Fintech Office collects information to support FHFA in making informed decisions, addressing emerging risks, and advancing mission priorities as they relate to housing finance fintech and innovations. The FHFA Ethics Office may review financial information to ensure that applicants/prospective participants do not have conflicts or issues that may disqualify them from working with FHFA and will then inform Fintech of the results of that review. However, none of the information reviewed or relied upon by the FHFA Ethics Office is provided or otherwise made available to the Fintech Office.
1.4	How is the information provided to FHFA?	The information in this system is collected directly from an individual or a representative of an entity via listening sessions, forums, office hours, and tech sprints. Members of the public may also submit information to the Fintech Office via email to fintech@fhfa.gov.

#	Question	Response
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, 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?	FHFA may review information to ensure that prospective participants do not have conflicts or issues that may disqualify them from working with FHFA. FHFA will in certain instances use the information collected to communicate and engage with interested individuals or entities on activities or initiatives hosted by the Fintech Office.
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 described in

#	Question	Response
		Section 6. 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?	The Division of Conservatorship Oversight and Readiness (DCOR) file plan will be updated to reflect that the National Archives and Records Administration (NARA) General Record Schedule (GRS) 6.2, applies to records in this information system even though this record schedule expressly applies to Federal Advisory Committee Act (FACA) committee records. Most of these records must be retained as permanent records for eventual transfer to NARA.
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.	GRS 6.2, Item 010 - Substantive Committee Records documenting the establishment and formation of committees and their significant actions and decisions – Permanent retention (transfer to NARA after 15 years). GRS 6.2, Item 020 - Substantive recordings of meetings and hearings not fully transcribed, captioned digital photographs, and related finding aids, of committee members and staff, meetings, or hearings – Permanent retention (transfer to NARA after 3 years). GRS 6.2, Item 060 - Committee Management Records created or maintained related to the overall management of the committee – Temporary – Destroy or delete after 3 years.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risk to an individual's privacy if the data is lost or compromised is identity theft, embarrassment, and/or misuse of the individual's personal information. To address these risks, access to Fintech information is limited to FHFA employees with an official business need-to-know.

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-5, Photographic, Video, Voice, and Similar Files; and FHFA-7, Mail, Contact, Telephone, and Other Lists.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Yes, at the time of registration for any fintech event, a Privacy Act Statement is presented to all members of the public who attend fintech listening sessions, forums, office hours, and tech sprints.
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?	Responses are voluntary.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals can direct requests for access to the Privacy Office 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?	The information collected could be shared with any FHFA office, including but not limited to the Office of Congressional Affairs and Communication. (OCAC), to facilitate the Fintech Office's planning activities.

#	Question	Response
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.	Subject to the applicability of routine uses described below in response to Question 5.3, information collected by Fintech 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.	Information from this System may be shared to external entities in accordance with the following routine uses: (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. (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, 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. (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 (e.g., federal, state, local, tribal, foreign or a financial regulatory

#	Question	Response
		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. (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.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	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 described in Section 6. 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 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.	The System Security Plan (SSP) for this information system describes how this system meets all National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 security controls including AC-2, Account Management.
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.	Help Desk staff and IT engineers with access to the information in this information system may consist of FHFA employees and contractor personnel. All users undergo personnel screening prior to gaining access to FHFA's network and are required to complete security and privacy awareness training within two weeks of their start date. Active Directory groups are used to apply permissions to all users based on the concept of least privilege. The Account

#	Question	Response
		Management Standard Operating Procedures (SOP) describes the procedures for using Active Directory (AD) groups to restrict access to information based on a user's business need.
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 is required 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?	The SSP for this information system describes the controls in place to protect the confidentiality, integrity and availability of data maintained within Fintech and transmitted across the network. Those controls include but are not limited to: - Multi-factor authentication for all privileged and non-privileged users; - Hard disk encryption on all FHFA workstations; - Layer-7 Intrusion Prevention System (IPS) and web-proxy; - Secure email filtering; - Einstein 3A protections; and - Always-on encrypted Virtual Private Network (VPN).
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Active Directory group policy changes are audited by Active Administrator and provided to IT engineers and IT security personnel in real-time.
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.	No SA&A is required for this system.

#	Question	Response
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?	No ATO is required for this system.