



**Privacy Impact Assessment Template**

**CORRESPONDENCE TRACKING SYSTEM**  
**(SYSTEM NAME)**

**March 2023**  
**Date**

## 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 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 purpose of the system is to capture and track correspondence that FHFA receives from external sources (the public, Congress, regulated entities, etc.). The system will capture information on the sender and nature of the correspondence (i.e. name; home and business address; email address; telephone numbers; and other contact information). The system will help ensure FHFA responds to the inquiry in a timely and accurate manner.

**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?	Information is collected about the individual who submits a letter, complaint, request, or inquiry (hereinafter "correspondence"), or on his/her behalf by a congressional representative and the issue or question raised. Data elements collected include name, address (home and/or business), email address (home and/or business), telephone number (home and/or business), and other personal or business information voluntarily submitted.
1.2	What or who are the sources of the information in the System?	The sources of information are the public, Congress, the government sponsored enterprises (GSEs), FHFA staff, other federal agencies, and state and local governments.

#	Question	Response
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information is received and collected in order for FHFA to respond to incoming correspondence. The system also tracks who is responsible for creating or responding to the incoming correspondence and attendant deadlines.
1.4	How is the information provided to FHFA?	Information is collected directly from the individuals who submit correspondence via email, U.S. postage mail, Express mail, voicemail, website forms, and facsimiles.
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.	There are some risks associated with information being handled by FHFA employees. While all employees are held accountable for any mishandling of PII, access will be limited to program office areas only and the system will allow users to restrict access down to certain individuals, if necessary. Since FHFA does not require PII data from individuals and in fact discourages them from submitting this type of information, risks to an individual's privacy are low. However, there are cases in which an individual may voluntarily choose to send PII to FHFA. In those cases, FHFA takes additional steps to ensure that the risks to the individual's privacy remain low by further limiting access to this 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?	To manage incoming and outgoing correspondence, and to expedite responses to Freedom of Information Act requests, Congressional subpoenas or document requests, Government Accountability Office (GAO) requests, and OIG requests. Information is also used to inform FHFA personnel, the GSEs, and/or FHFA Office of Inspector General (OIG) personnel about trending correspondence issues.
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.	The system is controlled by users who have been trained to input data into the system. The system tracks all user activity and reports what records were accessed and what actions were taken. Staff can only access the system when logged into the FHFA network using their username and password. Only system administrators can delete information.

### 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?	Seven years for consumer records and public inquiries. Permanent retention for Congressional inquiries.
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.	Yes. FHFA has established a retention schedule for consumer (Comprehensive Records Schedule [CRS] 1.5), congressional (CRS 1.2), and public inquiry records (CRS 1.6). See FHFA Comprehensive Records Retention Schedule.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risk is low since FHFA only retains the consumer and public information for seven years and the type of the information collected. Potential risks to an individual’s privacy if the data is lost or compromised could include identity theft, embarrassment, and/or misuse of the individual’s personal information.

### 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-3, Correspondence Tracking System (81 FR 11268) (March 3, 2016)
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Yes. Notice is provided via the FHFA Website Privacy Policy available on FHFA's website.
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?	Yes. All submissions to FHFA are voluntary.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	The SORN and FHFA's Privacy Act regulation (12 CFR Part 1204) provide procedures for individuals to request access and to amend or correct their information.
4.5	What are the procedures for correcting inaccurate or erroneous information?	See response to Question 4.4.

## Section 5.0 Sharing and Disclosure

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

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	Depending upon the nature of the correspondence, the information may be shared with FHFA personnel in various offices, including but not limited to the Office of the Director (OD), Office of Congressional Affairs Communications (OCAC), Office of General Counsel (OGC), Division of Housing Mission and Goals (DHMG), Division of Bank Regulation (DBR), Division of Enterprise Regulation (DER), and Division of Conservatorship Oversight and Readiness (DCOR). Generally, information is shared for the purpose of informing personnel of a complaint or issue or requesting assistance or input in responding to the individual.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	Depending upon the issue, information may be shared with an FHFA regulated entity and/or the FHFA OIG. FHFA may also forward correspondence that does not fall within FHFA's purview to other federal agencies when appropriate. The purpose of sharing the information is to inform the recipient, and to allow the recipient to review, analyze and take action, if appropriate. Generally, FHFA does not disclose PII to external parties. However, sometimes, in order to provide an external party with the relevant information (such as an address or other contact information necessary to respond to the communication), FHFA may have to share PII with that external party.

5.3	Is the sharing of PII outside the agency compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	Generally, PII is not shared but when it is shared, the PII is limited to only that which is sufficient to allow for an understanding of the complaint/inquiry and to initiate action, if appropriate. For consumer complaints and Congressional inquiries dealing with constituent matters, the PII typically shared consists of the complainant's (and/or borrower's) name, contact information and mortgaged or REO property address. Such sharing is compatible with the original information collection and is covered by an appropriate routine use in the FHFA-3.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	Generally, PII that FHFA provides to external persons, agencies, or other entities is the same information the FHFA regulated entity has on its system or has ready access to via the lender or servicer. Therefore, the risks arise from the transmission of the information rather than the information itself.  FHFA limits its transmission to specific individuals or units at FHFA OIG, GSEs, and other federal agencies using secure transmission methods, such as secure file transport protocol (SFTP). FHFA requests and receives an acknowledgment of receipt of the information to ensure that proper party received the information.

## 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?	Designated staff are granted read-only access to the system with limited access to their program office records only. User access is granted to only those who have been trained to enter data into the system. Internal procedures can be found on FHFA's intranet. For consumer items, users are limited to DCOR (admin) and OCAC and DER (read-only). The Policies Related to Consumer Communications and Consumer Communications Procedures can be found on FHFA's intranet.

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?	Potentially, depending on the nature of their assigned duties. System owner will grant access accordingly with the same rules and access privileges as FHFA employees.
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?	Training will be given to all administrative staff and other program office staff according to their assigned duties as it relates to managing agency correspondence. After initial training, an online training module will be available to staff and new employees.
6.4	Describe the technical/administrative safeguards in place to protect the data?	The system tracks and documents who accesses the system and when, and any changes that are made.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	An audit report is generated on a weekly basis and given to the system owner for review.
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 most recent ongoing SA&A including CTS was signed September 29, 2022.
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?	March 31, 2016