Privacy Impact Assessment Template

COMMUNITY SUPPORT PROGRAM SYSTEM
(System Name)

June 2023
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**
Michael Price	Michael.Price@fhfa.gov	DHMG/OHCI	(202)649-3134
Shannon Fountain (Back-Up Owner)	Shannon.Fountain@fhfa.gov	Office of Housing and Community Investment	(202) 649-3501

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 Federal Home Loan Bank Act [12 U.S.C. § 1430(g)] requires the Federal Housing Finance Agency (FHFA) to establish a Community Support Program for members of the Federal Home Loan Banks (Banks). Community Support Program regulations [12 C.F.R. part 1290] set forth standards of community investment or service for members of Banks to maintain continued access to long-term advances and to community investment products (i.e., Affordable Housing Program (AHP) and other Community Investment Cash Advances (CICA) programs). In addition, the regulation sets forth the process that FHFA follows in reviewing, evaluating, and communicating each member's Community Support performance.

The Community Support Program considers the member's performance under the Community Reinvestment Act of 1977 (CRA) and the member's record of lending to first time homebuyers. With certain limited exceptions, each Bank member must meet the CRA standards and the first-time homebuyer support standards set forth in the Community Support Program regulation. The Community Support Program requires Bank members to submit a Community Support Statement to FHFA once every two years (i.e., 2019, 2021, 2023 etc.). The Community Support Statement documents a Bank member's CRA performance and support of first-time homebuyers. A Bank member must provide to FHFA: (1) its CRA rating, if it is subject to the CRA, and (2) information about its support for first-time homebuyers.

Since the inception of the Community Support Program, Bank members were required to submit their Community Support Statement to FHFA every two years (i.e., over 6,000 Bank members manually completed and submitted every two years) for review. In 2016, the Office of Housing and Community Investment (OHCI) within the Division of Housing Mission and Goals developed an online electronic Community Support Statement which launched April 2017. The purpose of the Community Support Program is to collect, store, and review Community Support Statement information.

The online Community Support Statement must be completed and submitted by an appropriate senior officer of a Bank member institution. The statement also requires information about the Bank member's senior officer (name, work title, and work email); the institution's federal CRA rating, if applicable; and the institution's lending volume or other activities or investments supporting first-time homebuyers.

OHCI is the Community Support Program's system owner. Bank members should use this online system to submit their Community Support Statements to OHCI. OHCI will review each member's Community Support Statement to determine if a Bank member meets Community Support Program standards. Each Bank will notify its members of their Community Support Statement review results.

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?	Bank members' senior officers' (submitter) name, work title, and business email, which is all set forth in the Community Support Statement (060 Form); Bank members' contact information; data on their CRA performance, if applicable; and data on members' compliance with the First Time Homebuyer requirement.
1.2	What or who are the sources of the information in the System?	Members of Federal Home Loan Banks.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	To discharge FHFA's duties regarding the Community Support Program as set forth by the Federal Home Loan Bank Act [12 U.S.C. § 1430(g)] and by federal regulations [12 C.F.R. part 1290]. The Community Support Program requires the name, title, and business email of the individual submitting the Community Support Statement. That information must be submitted by an appropriate senior officer of the member bank. The submitter's information is used to send an email notice to the member acknowledging receipt of the Community Support Statement submission.
1.4	How is the information provided to FHFA?	Members enter the information through the Community Support Statement website, or they can submit a completed Community Support Statement (Form 060) by FAX or email to FHFA.
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 privacy risk is low because the PII (the name, title, and email address of a member's senior official) are likely publicly available on other platforms. The risk to an individual's privacy if the data is lost or compromised could consist of identity theft and/or misuse of the individual's PII.
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 will use the information to verify members' compliance with Community Support Program requirements, as set forth in the Federal Home Loan Bank Act [12 U.S.C. § 1430(g)] and in federal regulation [12 C.F.R. part 1290].
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 persons able to see the information have a need to know. Bank personnel and contractors accessing the information must submit a written request for access to FHFA. This document is signed and dated by each Bank's designated Community Support Program contact person. The users are granted access and permission levels according to their role issued by the Community Support Program Administrators. Banks and bank contractors have read-only access. Each approved user has a unique username and password issued by FHFA, and FHFA provides the user with a document specifying how to use the system.

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?	30 years.
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's Comprehensive Records Schedule (CRS) Item 2.3b - Supervision and Housing Mission - Electronic Systems Records (30-years).
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The information is retained in the Community Support Program system (or its next-generation upgrade) and made accessible as needed for 30 years in accordance with FHFA's CRS Item 2.3.b. Retention is consistent with other FHFA mission-related 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.	No. A SORN is not required because the information retrieved does not constitute a record under the Privacy Act.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	The Community Support Program Statement requests the Bank member institution submitter's name, title, and email address. The Bank member is submitting the statement directly to FHFA for review. A Privacy Act Statement is not applicable because records are not retrieved by a name or other personal identifier.
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?	Individuals representing the members may decline to provide the information sought by the Community Support Program System. However, FHFA will put the member on restriction, meaning that the member no longer has access to long term advances from the Federal Home Loan Banks and may not participate in certain mission programs of the Banks.
4.4	What are the procedures that allow individuals to gain access to their information?	The member submitter receives a .pdf copy of the information they provided.
4.5	What are the procedures for correcting inaccurate or erroneous information?	The member must submit a new Community Support Statement (Form 060) through the system.

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 Office of Technology and Information Management (OTIM) for purposes of maintaining and periodically modifying the system. Division of Bank Regulation (DBR) has access to assist with their examinations of the Banks. Office of General Counsel (OGC) may view data to provide legal advice to OHCI. Approved OTIM and DBR personnel may view all data in the system. OHCI might display part or all

		the data on an ad hoc basis to OGC to assist them in developing legal advice for OHCI.
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.	Information is shared with FHFA-approved personnel of the 11 Federal Home Loan Banks. Each Bank would have access to all data submitted by their members, but not the data submitted by members of other Banks. The Banks will have access to the submitter's name, title, and email address in order to communicate with the members. The Banks would also be able to view and download reports on the Community Support Program status of their members. The Banks could view training and legal materials housed on the system.
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, the external sharing of PII is compatible with the original purpose of this information collection set by the Federal Home Loan Bank Act [12 U.S.C. § 1430(g)] and by federal regulations [12 C.F.R. part 1290]. No SORN applies because no "system of records", as defined by the Privacy Act (5 USC 552a), is created.
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 consists of identity theft and/or misuse of the individual's personal information. The privacy risk is low because the PII (the name, title, and business email address of the senior Bank member official) is likely publicly available elsewhere.

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 persons able to see the information have a need to know. Bank personnel and contractors accessing the information must submit a written request for access to FHFA. This document is signed and dated by the Banks' designated Community Support Program contact person. The users have authorized access and permission levels, according to their role issued by the Community Support Program Administrators. Bank and Bank contractors have read-only access. Each approved user has a unique username and password issued by FHFA and FHFA provides them with a document specifying how to use the system. These procedures are documented in training materials FHFA provides to the Banks.

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?	Certain non-FHFA personnel will have access, as described in question 5.2. Bank and Bank contractors accessing the information must submit a written request for access to the system. This document is signed and dated by the Banks' designated Community Support Program contact person. The users are given access and needed permission levels according to their role issued by the Community Support Program Administrators. Bank and Bank contractors have read-only access. Each approved user has a unique username and password issued by FHFA and FHFA provides them with a document titled "FHFA Nextranet Portal Access Procedures" specifying how to use the system. Certain approved FHFA contractors may also access the system. OTIM staff submits a request to OHCI for contractors to be added, and OHCI adds them as approved users. The system displays a list of all approved users. OHCI and OTIM agree on a specific time when the access issued to the OTIM contractor(s) will be terminated.
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?	FHFA provides biennial training to the Banks via Teams, Zoom, or a similar system and using PowerPoint. Questions from the Banks are answered. The OTIM contractors are trained internally.
6.4	Describe the technical/administrative safeguards in place to protect the data?	As documented in the System Security and Privacy Plan (SSPP), access to the Community Support Program is limited to those with a business need to access the Community Support Program who have been approved for access by the System Owner. Role-based access controls are embedded in the design of the system, and users are granted the least privileged role required to carry out their responsibilities. The Community Support Program System is hosted by FHFA and accessible only to FHFA users with valid Active Directory accounts. Technical and administrative safeguards are documented within the SSPP and tested prior to authorization and annually thereafter, as part of FHFA's assessment and authorization (A&A) process and consistent with the NIST Risk Management Framework. These safeguards include, but are not limited to, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating and reviewing audit logs, data encryption, etc.

6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	On a biweekly basis, OTIM provides OHCI with a list of persons who have accessed the system. OHCI then verifies whether each person is an authorized user.
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 SA&A date is 7/14/2022.
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?	ATO was issued August 29, 2022.