Privacy Impact Assessment (PIA)

COMMUNITY SUPPORT PROGRAM SYSTEM

(Name of the Information System or Information Collection)

October 2025
Date

System/Collection Overview
Section 10(g) of the Federal Home Loan Bank Act requires FHFA to adopt regulations establishing standards of community investment or service for members of Banks to maintain access to long-term Bank advances (12 U.S.C. 1430(g)). Section 10(g) states that such regulations ‘‘shall take into account factors such as a member’s performance under the Community Reinvestment Act of 1977 (CRA) and the member’s record of lending to first-time homebuyers’’ FHFA’s current community support regulation (Community Support Program) implements section 10(g) at 12 CFR part 1290. The regulation details the CRA and first-time homebuyer standards that have been established pursuant to section 10(g). Each Bank member, except as provided in the regulation, must meet these standards to maintain access to long-term Bank advances. The regulation sets forth the process that FHFA follows in reviewing, evaluating, and communicating each member’s community support performance. The regulation also requires each Bank to establish and maintain a community support program that includes providing technical assistance to its members. The Community Support Program requires Bank members to submit a Community Support Statement to FHFA once every two years. 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. The purpose of the Community Support Program Portal 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 Bank members. 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. OAHCI is the Community Support Program’s system owner. Bank members use this online system to submit their Community Support Statements to OAHCI. OAHCI reviews each member’s Community Support Statement to determine if a Bank member meets Community Support Program standards. Each Bank notifies 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 System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	With respect to PII: Bank members’ senior officers’ (submitter’s) name, work title, and business email, which is all set forth on the Community Support Statement. With respect to other information: Bank members’ institutional contact information; data on their CRA performance, if applicable; and data on the members’ compliance with the first-time homebuyer requirement.

#	Question	Response
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	Senior officers of member institutions.
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 regulation (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. The information must be submitted by an appropriate senior officer of a member institution. 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 or otherwise obtained by the System/Collection?	Senior officers of Bank members enter the information through the Community Support Program portal via the web-based Community Support Statement.
1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) 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. • If no, state "N/A" in the response section.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	FHFA uses the information to verify members' compliance with Community Support Program requirements. The submitter's information is used to send an email notice to the member acknowledging receipt of the Community Support Statement submission.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Access to the information is restricted to those who require it for their official duties. Bank personnel and contractors accessing the information must submit a written request to FHFA for access to the Community Support Program Portal. 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 for their respective Bank. 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. These usernames and passwords are validated via FHFA's Active Directory system and are not stored in the Community Support Program Portal.

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 National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (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).

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 the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	No. A SORN is not required because the system does not constitute a "system of records" under the Privacy Act.
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	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 required because records are not retrieved by a name or other personal identifier.
4.3	Is an individual's response to the request for information voluntary or mandatory?	Voluntary. Individuals representing the members may decline to provide the information sought by the Community Support Program System.
4.4	What are the consequences if an individual declines to provide the information?	If a Bank member does not submit the required information, FHFA will put the member on restriction, meaning that the member no longer has access to Bank long-term advances and may not participate in certain mission programs of the Banks.
4.5	What are the procedures that allow individuals to gain access to their information?	The system is not subject to the Privacy Act and therefore there is no requirement to provide individuals with access to their PII in the system.
4.6	What are the procedures for correcting inaccurate or erroneous information?	This system is not subject to the Privacy Act and therefore there is no requirement to provide individuals with the ability to correct information. However, to correct or update information in a previous submission, the member may submit a new Community Support Statement with the correct or updated information through the Community Support Program Portal.

Section 5.0 Sharing and Disclosure

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

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	Information is shared with the Office of the Chief Information Officer (OCIO) for purposes of maintaining and periodically modifying the system. Division of Bank Regulation (DBR) employees have access to assist with their examinations of the Banks. Office of General Counsel (OGC) employees may view data to provide legal advice to OAHCI. Approved OCIO and DBR personnel may view all data in the system. OAHCI may display part or all data on an ad hoc basis to OGC to assist them in developing legal advice for OAHCI.
5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	Information is shared with FHFA-approved personnel of the 11 Banks. Each Bank has access to all data submitted by their members; however, it cannot access data submitted by members of other Banks. The Banks have access to the submitter's name, title, and email address to communicate with members. The Banks are also able to view and download reports on the Community Support Program status of their members. The Banks can also view training and legal materials housed on the system.
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes, the external sharing of PII is compatible with the original purpose of this information collection 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). There is no applicable SORN because the system does not constitute a system of records under the Privacy Act.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	Certain non-FHFA personnel will have access, as described in question 5.2. Bank employees and 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 employees and 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. OCIO staff submit a request to OAHCI for contractors to be added, and OAHCI adds them as approved users. The system displays a list of all approved users. OAHCI and OCIO agree on a specific time when the access issued to the OCIO contractor(s) will be terminated. Bank submitters also access the system by using the banks' identifiers through the system's website. These submitters can only access the webpage intended to submit information and then once submitted they are directed to a page where they must list their name, email, and title. These submitters cannot access other parts of the system at that time.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	There are no conflicts of interest with respect to the System or information.

#	Question	Response
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	FHFA provides biennial training to the Banks on how to use the Community Support Program system. In addition, all FHFA employees are required to undergo Security, Privacy, and Records and Information Management training at new employee onboarding training and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the regular collection, use, storage, access, or maintenance of PII.
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 FHFA users who access the system must have 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.

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	The privacy risk is low because the PII (the name, title, and business email address of a Bank 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, targeted phishing attacks, and/or misuse of the individual's PII.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Although the retention period for the information is relatively long (30 years), the risks associated with this length of time are low given the nature of the PII involved. Further, the risk of out-of-date information being utilized is low as members are required to submit information every two years, thereby providing a regular opportunity to provide updated contact information.
7.3	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 and is information that is likely routinely shared with the Banks in other contexts.