



Privacy Impact Assessment (PIA)

COMMUNITY SUPPORT PROGRAM SYSTEM
(Name of the Information System or Information Collection)

April 2026
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 the Federal Home Loan Banks (hereinafter referred to as “Bank members” and “Banks”, respectively) to maintain access to long-term Bank advances (12 U.S.C. 1430(g)). Section 10(g) states, in pertinent part, 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.” 12 C.F.R. 1290 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 regulation 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 Bank member senior officer. 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.

The Office of Affordable Housing and Community Investment (OAHCI) oversees the Community Support Program at FHFA. Bank members use the Community Support Statement website 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. OAHCI and Banks use the Community Support Program Portal to manage the Community Support Program. Each Bank notifies its members of their Community Support Statement review results.

Section 1.0 Characterization of the Information

The following questions address the scope of the personally identifiable information (PII) requested and/or collected. PII is information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII includes, but is not limited to, name, address, Social Security number, date of birth, financial information, and demographic information.

#	Question and Response
1.1	<i>What and whose PII is being collected, used, disseminated, or maintained?</i>

	<p>Bank representatives upload the name, work title, and business email to the Community Support Program Portal to authorize Bank members' senior officers to access the Community Support Statement website. Those senior officers provide the same PII when they submit the Community Support Statements (CSSs) on behalf of the Bank member they represent.</p>
<p>1.2</p>	<p><i>If Social Security Numbers (SSNs) are included, describe in detail:</i></p> <ol style="list-style-type: none"> <i>1) The business justification for collecting or using SSNs;</i> <i>2) The consequences if SSNs are not collected or used;</i> <i>3) How the SSNs will be protected while in use, in transit and in storage.</i> <p>This system does not collect SSNs.</p>
<p>1.3</p>	<p><i>How is the PII obtained? If individuals are not providing their own PII directly, describe where the information originates and any intermediaries it goes through before being provided to FHFA. Include a description of the mechanism by which the PII is provided to/obtained by FHFA.</i></p> <p>Senior officers of Bank members enter the information through the CSS website.</p> <p>Bank representatives authorized to access the Community Support Program Portal log into the portal via the FHFA Nextranet and upload a file or manually enter the details of individuals representing Bank members that are authorized to access the CSS website and submit a CSS.</p>
<p>1.4</p>	<p><i>How will the PII be used and for what purpose?</i></p> <p>This system collects PII 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). 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 CSS submission. This system also collects PII to: (1) define and authenticate individuals who are authorized access the CSS website and submit CSSs; and (2) implement multi-factor authentication, requiring designated members to input a verification code sent to their emails to access the CSS website and submit a CSS.</p>

1.5	<p><i>Is there a risk that PII other than that described above will be collected? If no, explain why not. If yes, explain the risk and how the risk is mitigated.</i></p> <p>There is a low risk that this system will collect PII other than that described above. The required credential information is predetermined and limited to that which is needed for authentication purposes. As for the PII on a member's submitted CSS, only the name and business contact information for a Bank member's representative is requested and generally that is all that is provided. It is possible that a member/member representative could add additional PII not required by the questions in the CSS, but this is unlikely to occur.</p>
1.6	<p><i>Is there a risk that the PII collected will be inaccurate? If no, explain why not. If yes, explain the risk and how the risk is mitigated.</i></p> <p>There is a low risk that PII collected by this system will be inaccurate. For purposes of the credential PII collected, inaccurate PII will prevent a Bank member's access to the CSS website and if such a circumstance occurred, the member would likely contact FHFA to restore access and accordingly correct any inaccurate PII. With respect to the PII collected via the CSS, Bank members are incentivized to provide accurate business contact information to ensure the CSS is accepted and FHFA can contact the identified representative to address any potential issues. To the extent any such PII in the CSS is inaccurate or needs to be updated, the Bank member can submit a new CSS with the correct or updated information through the CSS website to correct it. The Banks and FHFA can also correct inaccurate or outdated information via the Community Support Program Portal.</p>

Section 2.0 General

The following questions address general information about the information in the system, including how the information will be used and for what purpose.

#	Question and Response
2.1	<p><i>What is the legal authority for the collection?</i></p> <p>12 U.S.C §1430(g) (Advances to members: Community support requirements) and 12 CFR part 1290 (Community support requirements)</p>
2.2	<p><i>Is the collection of information subject to the Paperwork Reduction Act? If yes, what is the OMB Control Number for the collection?</i></p>

	Yes, this collection has been assigned OMB Control Number 2590-0005.
2.3	<p><i>Is this a new PIA or an update to an existing PIA?</i></p> <p>Update to an existing PIA.</p>
2.4	<p><i>Is the system internally operated or operated by a third-party (e.g., contractor)? If not internally operated, please identify the third party.</i></p> <p>This system is internally operated.</p>
2.5	<p><i>How is the risk of improper use of the PII by FHFA employees/contractors mitigated? If PII is shared with third parties, how will the risk of improper use by those parties be mitigated?</i></p> <p>The risk of improper use of system PII is low. Access to the information is restricted to those who require it for their official duties. Bank personnel 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 Bank users are granted access and permission levels according to their role issued by the Community Support Program Administrators. Banks have read-only access to information that members submit in the CSS for their respective Bank. Banks can edit the list of designated individuals representing member institutions, which does not affect any data in submitted CSSs. Each approved Bank user has a unique username and password issued by FHFA, and FHFA provides the Bank 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.</p> <p>In addition, the PII collected and used, i.e., name, title, and business email address of Bank member senior officials, is likely available to the public and is information that is likely routinely shared with the Banks in other contexts.</p>

Section 3.0 Retention

The following questions address how long PII will be retained after the initial collection.

#	Question and Response
---	-----------------------

3.1	<p><i>How long is the PII retained?</i></p> <p>30 years.</p>
3.2	<p><i>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.</i></p> <p>Yes, FHFA’s Comprehensive Records Schedule (CRS) Item 2.3b - Supervision and Housing Mission - Electronic Systems Records (30 years) applies to this system.</p>

Section 4.0 Notice, Individual Access, and Correction

The following questions address notice to the individual, the individual’s right to consent to uses of the PII, the individual’s right to decline to provide PII, and the individual’s ability to ensure the accuracy of the PII collected about them.

#	Question and Response
4.1	<p><i>Is information about an individual retrieved by an individual’s name or personal identifier such as name, email address, or date of birth? If yes, identify the applicable System of Record Notice (SORN).</i></p> <p>No. A SORN is not required because the system does not constitute a “system of records” under the Privacy Act.</p>
4.2	<p><i>How is notice about the collection of PII provided to an individual prior to collection from that individual? If notice is not provided, explain why.</i></p> <p>The CSS requests the Bank member 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.</p>
4.3	<p><i>Is an individual’s response to the request for PII voluntary or mandatory?</i></p>

	The request is voluntary.
4.4	<p><i>What are the consequences if an individual declines to provide the requested PII?</i></p> <p>Members’ representatives may decline to provide the required authenticating information to gain access to the Community Support Statement website, but members will then lose access to the website. Members may also decline to provide the information requested in the CSS form, but those members would then be prevented from accessing Bank long-term advances.</p>
4.5	<p><i>What are the procedures that allow individuals to gain access to their PII?</i></p> <p>The system is not subject to the Privacy Act. Therefore, there is no requirement to provide individuals with access to their PII in the system. Notwithstanding, FHFA Bank members’ representatives can access their data submitted via a CSS by using their credentials to access the CSS website.</p>
4.6	<p><i>What are the procedures for individuals to correct or update information about them?</i></p> <p>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 CSS with the correct or updated information through the Community Support Statement website. In addition, Banks and FHFA may correct information using the Community Support Program Portal.</p>

Section 5.0 Sharing and Disclosure

The following questions address the content, scope, and authority for sharing PII.

#	Question and Response
5.1	<i>Is PII shared with other offices or divisions within FHFA? If yes, identify the other offices/divisions and describe the purpose of or business need for sharing the PII.</i>

	<p>Information is shared with the Office of the Chief Information Officer (OCIO) for purposes of maintaining and periodically modifying the system. The 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.</p>
5.2	<p><i>Is PII shared with individuals or entities outside of FHFA? External entities include other Federal agencies, state or local governments, regulated entities, FHFA-OIG, and Congress. External entities do not include FHFA contractors that receive PII as needed in their performance of work for FHFA.</i></p> <p><i>If yes, please identify the PII shared, and for what purpose or business need.</i></p> <p>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 Bank 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.</p>
5.3	<p><i>If PII is shared with external entities, describe how the information sharing is compatible with the purpose for which the PII was collected.</i></p> <ul style="list-style-type: none"> <i>• If a SORN applies, identify the applicable routine uses in the SORN listed in Section 4.1.</i> <i>• If a SORN does not apply, describe 1) whether notice of the PII sharing was provided and if so, how; and 2) how the sharing of PII is consistent with the purpose for which the information was collected. Sharing with Congress, FHFA-OIG or the Government Accountability Office pursuant to the statutory authorities of those entities need not be addressed.</i> <p>There is no applicable SORN because the system does not constitute a system of records under the Privacy Act. Notice of the sharing of PII is provided by this PIA and is implicit in the use of the system. 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) as the information is necessary to effectively implement the program.</p>
5.4	<p><i>Describe how the risk of intentional or inadvertent disclosure of PII by FHFA employees/contractors is mitigated. (Address both disclosures within FHFA and disclosures to external parties.)</i></p>

	<p>Access is restricted to authorized personnel ensuring employees access only the minimum data necessary for their duties. The risk of improper disclosure is further mitigated by providing training to FHFA employees/contractors with respect to protecting PII.</p>
5.5	<p><i>If PII will be shared with external parties, describe how the risk of improper disclosure of the information by individuals or entities outside of FHFA is mitigated.</i></p> <p>External party access is restricted to those who require it for their official duties, as described in Section 2.5. Further, the risk of harm from any improper disclosure is low given the non-sensitive nature of the PII in the system.</p>

Section 6.0 Technical Access and Security

The following questions address technical safeguards and security measures.

#	Question and Response
6.1	<p><i>Will individuals other than FHFA employees and FHFA contractor personnel performing official FHFA duties have access to the system containing the PII? If yes, how will access to the system be granted and controlled with respect to these external parties?</i></p> <p>Certain non-FHFA personnel will have access, as described in Section 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 documentation specifying how to use the system.</p> <p>Senior officials of Bank members who submit information also access the system by using an authorized email address and the Bank member's 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.</p>
6.2	<p><i>Is any system-specific training or guidance related to PII or privacy provided to users of the system? If so, please describe.</i></p>

	Not applicable.
6.3	<p data-bbox="232 394 1143 426"><i>Describe the technical/administrative safeguards in place to protect the PII.</i></p> <p data-bbox="232 485 1446 846">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.</p>