Privacy Impact Assessment (PIA)

SUSPENDED COUNTERPARTY PROGRAM SYSTEM

(Name of the Information System or Information Collection)

November 2025
Date

System/Collection Overview
The Suspended Counterparty Program (SCP) System (System) is an existing, internally developed system, operated by the Federal Housing Finance Agency (FHFA) and used to manage the SCP. The System serves as a repository of reports/referrals submitted by the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), and the eleven Federal Home Loan Banks (collectively, the regulated entities). The regulated entities are required to report to FHFA when they become aware that an individual or institution, including any affiliates thereof, has potentially engaged in covered misconduct as defined in 12 CFR § 1227.2, if the individual or institution has been involved in a covered transaction with the regulated entity within the past three years. In addition to serving as a repository for information, the System is used to manage and track referrals from receipt through resolution. The system also collects information from other organizations and entities, including the FHFA Office of Inspector General (OIG), U.S. Department of Housing and Urban Development, other federal and state agencies, and members of the public, that voluntarily submit reports and referrals to FHFA about counterparties that have potentially engaged in covered misconduct as defined at 12 CFR § 1227.2. The system may also contain information provided by individuals or entities in response to their proposed suspension or in an appeal of their suspension. Under the SCP, FHFA may share information in the System with the regulated entities, state and federal housing or financial regulators, and state and federal professional licensing agencies.

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, and financial information.

#	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?	Information about counterparties and their affiliates is provided to the SCP. Information may include name, alternative name, address, Social Security number (SSN), state driver's license number, professional license number, date of birth, description of covered misconduct, description relationship with any affiliates, online profile, and account information. Information may also include the name and contact information of individuals submitting the report to FHFA or of individuals representing parties who have been suspended or proposed for suspension.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	Information is provided by FHFA OIG, Fannie Mae, Freddie Mac, the Federal Home Loan Banks, other Federal agencies, state agencies, and members of the public. Individuals or entities proposed or suspended may also submit information to the SCP in response to their

		proposed suspension or in an appeal of their suspension.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The collected information is necessary to fulfill the requirements at 12 CFR part 1227 and to ensure the safe and sound operation of the regulated entities, including addressing the risk to the regulated entities presented by individuals and entities with a history of fraud or other financial misconduct, pursuant to 12 U.S.C. §§ 4513 and 4526.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	The information is submitted electronically or by mail to the SCP address, the program manager for the SCP, or the Director of FHFA.
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.	Yes. SSNs are collected only as necessary so FHFA can confirm that a party referred to the SCP has or is currently doing business with a regulated entity and to avoid the risk of misidentification. SSNs, including files and electronic messages containing SSNs and other PII, are encrypted within the System. The System also masks SSNs while the System is in use.

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?	The information is used to determine if the regulated entities should be barred from doing business with a counterparty pursuant 12 CFR part 1227.
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.	Records are safeguarded in a secure environment. Buildings where records are stored have security cameras and 24-hour security guard service. Computerized records are safeguarded through use of access codes and other information technology security measures. Paper records are safeguarded by locked file rooms, locked file cabinets, or locked safes. 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?	Information contained in the database will be kept in accordance with OGC's records management file plan which provides for the destruction/deletion of records 15 years after the project/activity/transaction is completed or superseded.
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, Item 4.4 Litigation and Administrative Hearing Records, in accordance with FHFA's NARA-approved Comprehensive Records Schedule and OGC's file plan.

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.	Yes, Suspended Counterparty Program System (FHFA-23).
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.	SORN FHFA-23 as well as this PIA provide public notice.
4.3	Is an individual's response to the request for information voluntary or mandatory?	Although the regulated entities are required to report potential covered misconduct to the SCP, any information received from individuals proposed for suspension or who have been suspended is provided voluntarily.
4.4	What are the consequences if an individual declines to provide the information?	Individuals proposed for suspension who do not respond to the proposed suspension are limited in their ability to challenge their suspension. Likewise, an individual who has been suspended who does not respond cannot appeal their suspension. However, as a practical matter, most of the PII about an individual is originally

		received via the referral process, not from the individual.
4.5	What are the procedures that allow individuals to gain access to their information?	Individuals may submit a Privacy Act request for access to their information to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Additional information regarding Privacy Act requests is available on FHFA's website Privacy page, located at https://www.fhfa.gov/about/privacy.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Individuals may submit a request to amend or correct records to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(d). Additional information regarding the amendment of records pursuant to the Privacy Act is available on FHFA's website Privacy page, located at https://www.fhfa.gov/about/privacy.

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.	Yes. Information may be shared with the Office of the Director, OGC, Division of Bank Regulation, Division of Enterprise Regulation, and Division of Housing, Mission and Goals. Recommendation letters regarding suspension prepared by OGC staff may be provided to these offices for select counterparties as determined appropriate by OGC.
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.	Yes. Information is shared with the regulated entities to confirm that a counterparty has conducted business with a regulated entity and to provide the regulated entity an opportunity to inform FHFA of any potential impact from the suspension of a counterparty. Information may also be shared with FHFA OIG, other Federal agencies, state agencies, and professional licensing associations to help FHFA determine whether suspension of a counterparty is appropriate and the appropriate scope of any suspension. Additionally, information may be shared to assist in similar determinations by other Federal or state agencies, or professional licensing boards.
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	Yes. The sharing of information is compatible with the purpose of the information collection. This is documented in SORN FHFA-23, routine uses 7, 12, 13, 14, and 15.

	Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	

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.	Contractor personnel may have access to the System and information contained therein. Access is granted via role-based permissions and is managed by the SCP manager.
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.	No.
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management 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 for those individuals whose work duties and responsibilities regularly involve the 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 System is limited to those with a business need to access the System and who have been approved for access by the system owner. Role-based access controls are designed into the system and users are granted the least privileged role required to carry out their responsibilities. The 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 within the authorization cycle thereafter as part of FHFA's assessment and authorization plan, 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, and data encryption.

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 information in the System includes sensitive PII, thereby increasing the risks to an individual's privacy. The risks to an individual's privacy if the data is lost or compromised include identify theft, blackmail, loss of future business or employment opportunities, embarrassment, and/or misuse of the individual's personal information. These risks are mitigated by limiting access to the System to those who have a need-to-know in the performance of their official duties. Further, information is protected as described in Sections 1.5, 2.2, and 6.4.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are risks associated with the retention of data given the relatively long retention period, which increases the risk of information being subject to a breach. To protect against this risk, computerized records are safeguarded through use of access codes and other information technology security measures, and 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. Records are likewise disposed of in accordance with FHFA's records retention schedule pursuant to standard policies/ procedures.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	There are risks associated with the external sharing of information in the System, including accidental disclosure to the incorrect party and further disclosure by third parties. However, the risks are mitigated by limiting any external sharing to that which is required in the discharge of FHFA's obligations under 12 CFR part 1227. System users receive role-based privacy training to reduce the risk of inadvertent disclosure. Third parties that receive PII or other types of Controlled Unclassified Information (CUI) are notified of the information's protected status via CUI document markings or other means.