



Privacy Impact Assessment Template

SUSPENDED COUNTERPARTY PROGRAM SYSTEM (SCP)
SYSTEM NAME

November 2022
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 |
| Crystal Miller | Crystal.Miller@fhfa.gov | Office of General Counsel (OGC), Administrative Law & Alternate Designated Agency Ethics Official (ADAEO) Branch | 202-649-3079 |
| | | | |
| <p>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.</p> <p>The purpose of the Suspended Counterparty Program System (SCP or the System) is to receive reports from the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), and the eleven Federal Home Loan Banks (the regulated entities) when they become aware that an individual or institution and any affiliates thereof, which are currently or have been engaged in a covered transaction with a regulated entity within three years of when the regulated entity becomes aware of the covered misconduct, have engaged in fraud or other financial misconduct.</p> <p>The system also collects information from other organizations and entities besides the regulated entities that voluntarily submit reports to the Federal Housing and Finance Agency (FHFA) about counterparties that have engaged in covered misconduct as defined at 12 CFR 1227.2.</p> <p>Under the SCP, FHFA intends to share information in the system with the regulated entities, state and federal housing or financial regulators, and state and federal professional licensing agencies.</p> | | | |

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 about counterparties is provided to the SCP. This includes name, alternative name, address, social security number (SSN), state driver's license number, professional license number, date of birth, description of covered misconduct as defined in 12 CFR 1227, affiliate information (name, address, professional license number or other identifying information, description of how the affiliate is related to the subject), online profile and account information. |
| 1.2 | What or who are the sources of the information in the System? | FHFA Office of Inspector General (OIG), Fannie Mae, Freddie Mac, Federal Home Loan Banks, Federal agencies, state agencies, and members of the public. |

| # | Question | Response |
|-----|---|--|
| 1.3 | For what purpose is the information being collected, used, disseminated, or maintained? | This information is necessary to fulfill the requirements at 12 CFR 1227. Social Security numbers (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. Without SSNs, it would be extremely difficult to determine if a party referred to the SCP is doing or has done business with a regulated entity. The collection of this information is necessary to ensure safe and sound operation of the regulated entities and prevent fraud upon the regulated entities, pursuant to 12 USC 4513, 4515 and 4526. |
| 1.4 | How is the information provided to FHFA? | This information is submitted electronically or by mail to the SCP address, the program manager for the SCP, or the Director of 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 risk to an individual's privacy if the data is lost or compromised is identify theft, blackmail, loss of future business or employment opportunities, embarrassment, and/or misuse of the individual's personal information. |
| 1.6 | Are Social Security numbers are being collected or used in the system? | Yes. |
| 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. | 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. Without SSNs, it would be extremely difficult to determine if a party referred to the SCP is doing or has done business with a regulated entity. The collection of this information is necessary for the safe and sound operation of the regulated entities pursuant to 12 USC 4513, 4515 and 4526. If SSNs are not collected, FHFA will not have sufficient information on which to initiate and complete an investigation of the allegations. SSNs are |

| | | |
|--|--|---|
| | | encrypted within the database interface. Files and electronic messages containing SSNs and other personally identifiable information are encrypted. Furthermore, SSNs are used in accordance with the FHFA Procedures for Determining Whether Any New Collection or Use of Social Security Numbers Is Necessary (May 2019). |
|--|--|---|

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? | Information is used to determine if the regulated entities should be barred from doing business with a counterparty on the Suspended Counterparty list. If so, information will also be used to determine the appropriate length of suspension. |
| 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. | Records are safeguarded in a secured 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 2022 OGC records management file plan. |
| 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. | The retention schedule is in accordance with the 2022 OGC records management file plan. |
| 3.3 | Discuss the risks associated with the length of time data is retained and how those risks are mitigated. | The risk to an individual's privacy if the data is lost or compromised is identify theft, blackmail, loss of future business or employment opportunities, embarrassment, and/or misuse of the individual's personal information. |

| | | |
|--|--|---|
| | | To protect against those risks, 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. |
|--|--|---|

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. | Yes, Suspended Counterparty Program System (FHFA-23). |
| 4.2 | Was notice provided to the individual prior to collection of information? If so, what type of notice was provided? | No, information is obtained via required reports from the regulated entities or voluntarily from other organizations and entities about counterparties that have engaged in covered misconduct as defined at 12 CFR 1227.2. No information is collected directly from individuals. |
| 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? | No, information is obtained via required reports from the regulated entities or voluntarily from other organizations and entities about counterparties that have engaged in covered misconduct as defined at 12 CFR 1227.2. No information is collected directly from individuals. |
| 4.4 | What are the procedures that allow individuals to gain access to their information? | The procedures that allow individuals to gain access are set forth in the FHFA SORN, Suspended Counterparty Program System (FHFA-23). Individuals may submit a Privacy Act request to FHFA’s Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Instructions for submitting Privacy Act requests are available on FHFA’s website Privacy Page, located at https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx . |
| 4.5 | What are the procedures for correcting inaccurate or erroneous information? | The procedures that allow individuals to gain access are set forth in the FHFA SORN, Suspended Counterparty Program System (FHFA-23). Individuals may also submit a Privacy Act request to FHFA’s Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Instructions for submitting Privacy Act requests are available on FHFA’s website Privacy Page, located at |

| | |
|--|---|
| | https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx . |
|--|---|

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? | Office of the Director, OGC, Office of Conservatorship, Division of Bank Regulation, Division of Enterprise Regulation, Division of Housing, Mission and Goals, and Division of Accounting and Financial Controls Branch. Recommendation letters regarding suspension prepared by OGC staff will be provided to these offices for select counterparties referred to the SCP as determined appropriate by OGC. |
| 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. | The regulated entities, entities that referred a counterparty to FHFA and licensing boards. Information is shared with the regulated entities to confirm that a counterparty has done business with a regulated entity and to provide the regulated entities an opportunity to inform FHFA of any potential impact from the suspension of a counterparty. Information may be shared with FHFA Office of Inspector General (OIG), other Federal agencies, state agencies, and professional licensing associations to help FHFA determine whether suspension of a counterparty is appropriate and the appropriate level of any suspension. Information also 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 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. | The sharing of information with the regulated entities, state and federal housing regulators, and state or federal professional licensing agencies pursuant to routine uses 13, 14, and 15, respectively, as provided in SORN FHFA-23. |
| 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 is identity theft, blackmail, loss of future employment opportunities, embarrassment, or misuse of the individual's personal information. These risks are mitigated by limiting any external sharing to that which is required by law in the discharge of FHFA's obligations under 12 CFR Part 1227. In addition, all FHFA Non-Public Information, including Confidential Supervisory Information, is marked as CONTROLLED and all |

| | | |
|--|--|---|
| | | General Privacy or Personally Identifiable Information (PII) is marked as CONTROLLED//SP-PRVCY. |
|--|--|---|

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? | As detailed in the System Security and Privacy Plan (SSPP) for SCP, which is a FHFA “controlled” document, access to the SCP is limited to those with job responsibilities related to the SCP and for whom the SCP System Owner has approved such access in writing. All such approved personnel must be authenticated via the FHFA Active Directory for each attempted access to the SCP and must also be added to the SCP as a user with a user assigned role. Role-based access controls are designed into the SCP and applied through application controls that establish role-based permissions, whereby the regular user role is restricted from viewing or modifying administrative screens, such as those that allow modification of users and permissions. |
| 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? | Contractor personnel may have access to the System and information contained therein. They will gain access through a control panel that is managed by the SCP manager and staff in OTIM with a need to know. Procedures are located in the Controlled Unclassified Information (CUI) Procedures . |
| 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? | All FHFA employees are required to undergo security, privacy, and Records and Information Management (RIM) 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 involve the collection, use, storage, access, or maintenance of PII. |
| 6.4 | Describe the technical/administrative safeguards in place to protect the data? | Technical safeguards include encryption of personally identifiable information, least privilege user access, limited access to folders containing SCP information, an access log for those who have accessed the data, and those additional procedures set forth in the Guidance for Safeguarding and Destroying Controlled Unclassified Information (CUI) . |

| # | Question | Response |
|-----|--|---|
| 6.5 | What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed? | OTIM Security has created audit logs that will contain date of event, user, IP address, and a description of the event. Audit reports will be sent to the system owner on a monthly basis 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. | Yes, an A&A was last performed on August 22, 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? | SCP received its initial ATO on December 13, 2017 and remains in ongoing authorization. |