Privacy Impact Assessment (PIA) Template

GOOD FAITH EFFORT REVIEW SYSTEM
(Name of the Information System or Information Collection)

APRIL 2025
Date

Brent Burris
Senior Agency Official for Privacy
(202) 649-3037
Brent.Burris@FHFA.gov

System/Collection Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Catherine Chiang	Catherine.Chiang@fhfa.gov	OCOO	(202) 649-3122
Executive Sponsor			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Marcus Williams	Marcus.Williams@fhfa.gov	OCOO	(202) 649-3609

System/Collection Overview

Section 342(c) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) provides the authority for FHFA's Office of Minority and Women Inclusion's (OMWI's) Good Faith Effort (GFE) Reviews. Reviews are conducted for contractors whose contract contains the FHFA GFE contract clause (hereinafter, "covered contractors"). The review process is executed manually, predominantly via email. Also, reviews have been conducted using a sample of contracts versus all eligible contracts.

The Good Faith Effort Review system is a FHFA-operated system. The purpose is to execute the review process and ensure compliance with the Dodd-Frank Act more efficiently. The aim is to automate, to the extent practicable, the existing GFE Review process to enable more efficient execution and management.

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 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?	1. FHFA Contractor's name and address, Contractor POC's name, business email address and business telephone number; 2. The total number of Contractor's employees, and the number of minority and women employees, by race, ethnicity, and sex (e.g., the EEO-1 Report) or similar information; and 3. A list of subcontract awards under the Contract that includes dollar amount, date of

		award, and subcontractor's race, ethnicity, and/or ownership status.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	Covered contractors provide the information to the Office of the Chief Financial Officer (OCFO).
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The purpose is to review Contractor's compliance with Section 342(c) of the Dodd-Frank Act, codified at 12 U.S.C. § 5452(c).
1.4	How is the information provided to or otherwise obtained by the System/Collection?	Covered contractors provide the information to OCFO. OCFO then either provides the information to OMWI or enters the information directly into the system.
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?	The information will be used to review compliance with Section 342(c) of the Dodd-Frank Act.
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 this system is limited to agency employees who have a business need-to-know for the information.

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 is retained 7 years after cut-off when the project/activity/ transaction is complete.

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 Item 5.2 Budget and Financial Management Records.

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. However, OCFO collects this data pursuant to SORN No. FHFA-2.
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.	Notice is not provided because the system is not the original point of collection. OMWI receives the information from OCFO.
4.3	Is an individual's response to the request for information voluntary or mandatory?	N/A
4.4	What are the consequences if an individual declines to provide the information?	N/A
4.5	What are the procedures that allow individuals to gain access to their information?	Individuals can direct requests for access to their information to the Privacy Office in accordance with FHFA's Privacy Act Regulation, 12 CFR 1204, which is expressly referenced in SORN No. FHFA-2.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Individuals can direct requests to correct or amend their information to the Privacy Office in accordance with FHFA's Privacy Act Regulation, 12 CFR 1204, which is expressly referenced in SORN No. FHFA-2.

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.	The information is shared between OMWI and OCFO to confirm compliance with Section 342(c) of the Dodd-Frank Act.
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.	No.
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.	N/A

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.	No. Access to the system is limited to OMWI and OCFO. Written procedures in the System Security and Privacy Plan (SSPP) document how FHFA securely manages access to the system and assign permissions based on the concept of least privilege. Access privileges are certified annually.
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 (RIM) 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 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 SSPP, access to the Good Faith Effort Review 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 Good Faith Effort Review 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.

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 name and contact information for a Contractor's POC can be combined with other data to expose other potential PII. This risk is mitigated by limiting the information collected to that which is used to assess compliance with the Dodd-Frank Act and limiting the number of employees with access to this information system.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The data retention is a low risk. Data will remain in the system for 7 years. The risk is mitigated by limiting access to the those who have a business need-to-know the information.

7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	N/A