Privacy Impact Assessment Template

FAIR LENDING OVERSIGHT DATA SYSTEM
(SYSTEM NAME)

March 23, 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**
James Wylie	James.Wylie@fhfa.gov	DHMG/OFLO	
Jonathan Liles	Jonathan.Liles@fhfa.gov	DHMG/OFLO	

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.

The purpose of the fair lending oversight data system is to store, maintain, and analyze information for fair lending oversight of FHFA's regulated entities. The data system is used for compliance activities, policy analysis, and for storage of fair lending information shared with other agencies in certain circumstances.

The database system is a collection of independent sources of data from the regulated entities and data collected by other federal agencies that contain information on a borrower, a property, or a loan application. FHFA uses supervisory, regulatory, conservator, and other authorities to obtain the data on an ongoing basis as well as make as needed data requests.

The sources of data are used to analyze compliance with the Fair Housing Act, the Equal Credit Opportunity Act, and the Safety and Soundness Act. They are also used for policy analysis and conservator oversight of the Enterprises. Information is shared with other Federal agencies in certain circumstances.

The current Office of Fair Leading Oversight (OFLO) database system is located on DC-Modeling and Research System (DC-MARS) and follows FHFA IT security protocols, with limited access. The database system contains the following types of information:

- Information about borrower and loan characteristics such as credit score, closing costs, interest rates, income, race, ethnicity, sex, age, debt ratio, and loan amount;
- Information about loan transactions including mortgage loan originator identification numbers, originating lender identifiers, and seller identifiers;
- Information about loan payment history;
- Information about property characteristics obtained from appraisal and collateral reports such as appraised value, comparable properties, adjustments, involved in loan applications and transactions;
- Information about appraisers performing appraisal reports such as name and license number;
- Information about multifamily property transactions including information about parties involved in the transaction including names, property addresses, and transaction underwriting characteristics;
- Information about real-estate owned properties such as appraised values, condition, repair status, and property address;
- Information about automated underwriting system loan applications including property address and borrower and loan characteristics and automated underwriting system results;
- Data collected from Office of Fair Lending Oversight reporting orders 2021-OR-FHLMC-2 and 2021-OR-FNMA-2;

- HMDA regulator data provided by the Consumer Financial Protection Bureau (CFPB) to FHFA for fair lending purposes;
- Individual complaints related to fair lending oversight issues received from the Department of Housing and Urban Development (HUD), other FHFA offices, FHFA Office of Inspector General (OIG), or other sources; and
- Other information about applicants, properties, borrowers, and loan transactions obtained as part of OFLO oversight.

In some cases, these data elements are sourced from other agency data collections with appropriate controls.

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?	The data system contains information on race, ethnicity, age, gender, Government ID number (National Mortgage Loan Identification System) loan originator ID number, appraiser registry ID number, home/business address and telephone number, mortgage loan number and geolocation data, among others.
1.2	What or who are the sources of the information in the System?	The data stored is sourced from other offices/components within FHFA, the regulated entities, HUD, the CFPB, and the Federal Home Loan Banks – data is used as authorized by delegated authority or use agreements with other agencies.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information is being collected and analyzed for fair lending compliance, investigative, enforcement, policy analysis, and supervisory reviews conducted by OFLO. The information is shared with other federal fair lending and fair housing regulators in certain circumstances for fair lending and fair housing investigation, supervision, and enforcement purposes.

1.4	How is the information provided to FHFA?	The mode of data transfer is via Secure File Transfer Protocol (SFTP). FHFA's Office of Technology and Information Management (OTIM) receives the data from the server and stores it in the appropriate directory with UNIX access controls.
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.	Borrower and loan characteristics such as credit score, income, race, ethnicity, debt ratio, loan amount, etc. are contained in the Fair Lending Oversight Data System. The geographical location information is stored (separately) in the form of latitude, longitude, street address, and Census tract. The information could be merged by location with publicly available data to obtain proprietary loan and credit information for a particular address.
1.6	Are Social Security numbers are being collected or used in the system?	No.
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.	N/A

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?	OFLO and other authorized users use the database system for supervision of the regulated entities with respect to compliance with applicable fair lending law and other agency policy and supervisory purposes. The datasets are used for conducting compliance reviews, analyzing impact of proposed or existing policy, monitoring, reporting, and general research. The data is also used to identify mortgage interest rate disparities of primary market

		lenders. The information is shared with other federal fair lending and fair housing regulators in certain circumstances for fair lending and fair housing research, investigation, supervision, and enforcement purposes.

#	Question	Response
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.	FHFA's OTIM Help Desk grants access to fair lending data directories on DC-MARS for those who have a need to know. The OTIM Help Desk requires approval by the manager of the employee and owner of the directory to grant access. This structure limits access to the OFLO UNIX group and OFLO is responsible for approving access. UNIX permissions control access within directories, based on the owner and group-level access. OFLO also requests PII data elements to be contained in separate datasets within subdirectories. Data obtained from existing datasets within FHFA is used in accordance with delegated authority.

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 pursuant to OFLO and the Division of Housing Mission and Goals (DHMG) file plans, which maintains certain records permanently, some for 30-year retention, and some for 7-year retention.
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.	Items 2-2.2 Supervision and Oversight Activities Records (including b, c, d, and f) in DHMG's file plan covers the records associated with this system.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	**Risk:** Long retention periods pose a risk that information can be accessed long after collection. **Mitigation:** Limit user access and provide training on data use and record retention.

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.	No. However, a SORN will be needed. SORN name: Fair Lending and Oversight Data System Project Publication data: April 2022
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	No, the information is collected from third Parties (e.g., the regulated entities, other agencies, other FHFA offices). For race, ethnicity, age, and sex data, mortgage applicants are provided a notice of the information being collected and its purposes. For appraisal data, the Uniform Residential Appraisal Report (URAR) provides notice that the report may be shared with federal agencies without obtaining the appraiser's permission.
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?	Generally no, since the information is collected from third parties (*e.g.,* the regulated entities, other agencies, other FHFA offices) not directly from OFLO. However, for application and loan data about race, ethnicity, sex, and age, mortgage applicants may choose not to provide the information, subject to a requirement that loan officers collect the information based on visual observation or surname in certain cases where the borrower chooses not to provide it (see 12 CFR 1003, appendix B).
4.4	What are the procedures that allow individuals to gain access to their information?	See Fair Lending and Oversight Data System SORN.
4.5	What are the procedures for correcting inaccurate or erroneous information?	See Fair Lending and Oversight Data System SORN.

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?	Data is shared with members of DHMG, DER (Division of Enterprise Regulation), and DRS (Division of Research and Statistics) as necessary for compliance, supervision, policy, and research purposes.
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.	Non-public data is not shared with the public unless authorized by the Director pursuant to FHFA policies and requirements. The information is shared with other federal fair lending and fair housing regulators and other federal agencies in certain circumstances for fair lending and fair housing research, investigation, supervision, and enforcement purposes. For example, mortgage interest rate disparity data is shared with federal fair lending regulators annually under 12 U.S.C. 4561(d).
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.	Sharing of PII information is compatible with the original information collection. PII, such as address, is commonly shared as part of the HMDA regulatory file and used in fair lending analytics. Address data is collected by law under HMDA specifically for fair lending analysis, including redlining patterns. The URAR includes notice of nondiscrimination requirements and provides that the information may be shared with federal agencies.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	**Risk:** With sharing of appraisal and mortgage or other data, privacy risks to the individual include the identification of specific property attributes such as address. **Mitigation:** Privacy risks are mitigated with separation of PII and underlying data when shared with partner regulatory agencies.

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?	FHFA's OTIM determines access to the system. Permissions are governed based on UNIX group access on DC-MARS. Access to Fair Lending data group requires manager approver and owner of directory to approve access. UNIX groups are utilized to control access to each dataset residing on DC-MARS. Data owners approve all access to data sets under their control.
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?	No.
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, who have access to FHFA systems and records, are required to complete annual IT Security and Privacy awareness training.
6.4	Describe the technical/administrative safeguards in place to protect the data?	FHFA's OTIM determines access to the system. Permissions are governed based on UNIX group access. Access to Fair Lending data group requires manager approver and owner of directory to approve access. UNIX groups are utilized to control access to each dataset residing on DC-MARS. Data owners approve all access to data sets under their control.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	OFLO will work with OTIM to review access to the Fair Lending Oversight Data System. Reviews will be conducted per agency guidelines.
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.	These datasets are stored on the FHFA Analytics Platform which has undergone a SA&A and remains in ongoing authorization.

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?	The ATO for FHFA's Analytics Platform applies to these datasets.