Privacy Impact Assessment Template

FHFA ANALYTICS PLATFORM
(SYSTEM NAME)

DECEMBER 6, 2018
DATE

This template is used when the Senior Agency Official for Privacy determines that an IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the Senior Agency Official for Privacy.

David A. Lee
Senior Agency Official for Privacy
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024
(202) 649-3803
Privacy@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 IT System or project that collects, maintains, or disseminates PII from or about members of the public; or 2) initiates a new electronic collection of PII for 10 or more members of the public. System Owners are primarily responsible for completing the PIA with assistance from IT developers, IT security officers, and the Privacy Office.

Below is guidance, by section, for a System Owner to follow when completing a PIA.

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

This section provides an overview of the System and addresses 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.

Date submitted for review: December 6, 2018

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Tom Leach	Thomas.leach@fhfa.gov	OTIM	202-649-3640
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 FHFA Analytics Platform is comprised of multiple environments, databases and tools used by researchers and analysts for analyzing and processing historical and current housing data and for forecasting future trends and patterns. The Analytics Platform consists of public and private financial housing data submissions which are used for state and federal reporting, policy analysis, and decision-making. The FHFA Analytics Platform is comprised of the following components:

1. **Modeling and Research System (MARS):** MARS serves as the primary modeling and analysis platform used for data analytics. MARS provides access for FHFA economists, researchers and analysts to key datasets for which they have been granted access, and to a variety of software tools including SAS, SAS Enterprise Guide, Stata, SlickEdit, StatTransfer, and Oracle R.

The primary datasets residing on MARS include:

- Guarantee Fee
- Mortgage Loan Integration System (MLIS)
- Home Affordable Modification Program (HAMP)
- Home Mortgage Disclosure Act (HMDA)
- Housing Goals
- Housing Price Index (HPI)
- National Mortgage Database
- Loan Performance (LP)
- DataQuick Information Systems County Records Data
- DataQuick Assessor History
- Time Zero (TZ)

- FHA
- FHLBNY
- Mod_Pop
- Multiple Listings Service (MLS)
- Neighborhood Stabilization Initiative (NSI)

2. **Data Warehouse (DWS):** DWS consists of a collection of database schemas from datasets maintained on MARS. DWS is used to provide additional structure and access capabilities for researchers, economists and analysts.

   The primary datasets resident in the Data Warehouse include:

   - Guarantee Fee Database
   - Historical Loan Performance Database (HLP)
   - Mortgage Loan Integration System Database (MLIS)
   - Home Mortgage Disclosure Act (HMDA)
   - Loan Performance (LP)
   - Time Zero (TZ)
   - OpsRisk
   - FHA
   - Intex

3. **National Mortgage Database (NMDB):** The NMDB serves as a dedicated platform for external (non-FHFA) users of the NMDB project. Users of the NMDB are provided with access to analytical tools and NMDB data, and are restricted from accessing other FHFA resources.

4. **SFTP Servers**: Data used for analytics is in many cases delivered to FHFA by external sources over Secure File Transfer Protocol (SFTP). Separate Solaris zones have been established on a dedicated SFTP server for each data source (i.e. Freddie Mac, Fannie Mae, Treasury, etc.). The SFTP servers reside on the FHFA Demilitarized Zone (DMZ).

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?	FHFA collects and/or receives data from various sources described in the system overview. These datasets are used by FHFA analysts for modeling, research and forecasting, and are used to develop reports and data which are often shared publicly to increase the transparency in the housing finance markets and improve the public's understanding

#	Question	Response
1.2		of housing finance. Such data includes the House Price Index (HPI), the Foreclosure Prevention Report, the Refinance Report the Single Family Guaranteed Fees Report and more. Information varies by data sets. Cumulatively, data contained within the Analytics Platform includes fields such as: - Borrower characteristics ○ Gender ○ FICA score ○ Race/Ethnicity - Loan characteristics ○ Loan type ○ Loan amount ○ Loan identifier ○ Down payment ○ Loan to value ratio ○ Interest rate ○ Value ○ Servicer - Property characteristics ○ Address ○ Property type ○ Number bedrooms ○ Number bathrooms ○ Year built ○ Census tract
1.2	What or who are the sources of the information in the System?	Datasets are received from various sources, including Fannie Mae, Freddie Mac, Dept. of Treasury, FHA, VA, Experian, etc. Additional datasets that include aggregated public records are purchased from vendors.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The datasets are used by FHFA analysts for modeling, research and forecasting, and are used to develop reports and data which are often shared publicly to increase the transparency in the housing finance markets and improve the public's understanding of housing finance. Such data includes the House Price Index (HPI), the Foreclosure Prevention Report, the Refinance Report the Single Family Guaranteed Fees Report and more.

#	Question	Response
1.4	How is the information provided to FHFA?	Analytics Platform data sets are primarily delivered to FHFA via Secure File Transfer Protocol (SFTP) by the source of the data (e.g, Fannie Mae, Freddie Mac, Experian, Dept. of Veterans Affairs, Federal Housing Administration (FHA), etc.) while additional data sets are purchased from data vendors such as McDash, DataQuick, Core Logic, etc.
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 characteristics such as FICA score, income, ethnicity, etc. are contained in limited Analytics Platform data sets. While this data is not associated to a unique identifier such as name or SSN, if this data were associated to a property street address through a separate dataset, then an individual's income, FICA score and other financial information could be directly linked to the borrower.
1.6	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit and in storage.	N/A. SSNs are not collected.

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?	The datasets are used by FHFA analysts for modeling, research and forecasting, and are used to develop reports and data which are often shared publicly to increase the transparency in the housing finance markets and improve the public's understanding of housing finance. Such data includes the House Price Index (HPI), the Foreclosure Prevention Report, the Refinance Report the Single Family Guaranteed Fees Report and more.

#	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.	The FHFA office of Policy, Analysis and Research (OPAR) has developed a policy and specific procedures to minimize the extent to which actual street addresses are present and accessible in OPAR-controlled data files on the Analytics Platform. This includes running a program to mask street addresses in datasets, further restricting access to datasets that contain street addresses, and routinely reviewing users with access to data sets that contain street addresses.

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?	Data in FHFA mission systems is owned by business unit offices and generally retained for 30 years, but may be retained permanently if the data is determined to have broad industry-wide utility, public interest, or historical value.
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.	FHFA's Comprehensive Records Schedule (CRS) Item 2.3 - *Supervision and Housing Mission Electronic Systems Records* covers data contained within mission-related business systems, as well as the records that document the development and operation of those systems. **Item 2.3a:** Housing mission and industry data that represent compilations of information that may have broad industry-wide utility, public interest, or historical value – Disposition: PERMANENT. **ITEM 2.3b:** Mission-related data that is gathered and maintained for internal FHFA analysis and business purposes, and that are not released to the public due to the sensitive nature of the information – Disposition: TEMPORARY. Destroy or delete data 30 years after the system is retired.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	**Risk:** Challenge to manage data in an accessible format for 30 years after a system is retired. **Mitigation:** Generally, data is migrated into next generation systems as they are upgraded. In such instances, only information that is not

#	Question	Response
		migrated into the new system must be accessible for 30 years.

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.	A SORN has been completed for the National Mortgage Database, a component of the Analytics Platform: FHFA-21 National Mortgage Database System.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	No since the information is collected from third parties.
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 since s the information is collected from third parties.
4.4	What are the procedures that allow individuals to gain access to their information?	See the SORN FHFA-21 for National Mortgage Database System.
4.5	What are the procedures for correcting inaccurate or erroneous information?	See the SORN FHFA-21 for National Mortgage Database System.

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 sets residing on the Analytics Platform are used by various FHFA offices including the Division of Housing Mission & Goals (DHMG), the Office of Strategic Initiatives (OSI), the Division of Enterprise Regulation (DER) and the Division of Bank Regulation (DBR). Data sets are

#	Question	Response
		restricted and can only be accessed by users who have been specifically granted access by the data owner.
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.	NMDB data is shared with authorized individuals from the Consumer Financial Protection Bureau (CFPB), Fannie Mae, Freddie Mac, Federal Reserve, Department of Housing and Urban Development (HUD), Census and other federal agencies. All NMDB data resides within FHFA's network, but external users can securely access the data remotely via FHFA's Citrix environment.
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.	N/A. No PII is shared outside of the agency. All PII fields in the NMDB have been transposed with an encrypted PIN which is only known by Experian, the source of the data.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	N/A. No PII is shared outside of the agency.

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?	The Analytics Platform System Security Plan describes how the Analytics Platform meets all NIST SP 800-53 Revision 4 security controls including AC-2, Account Management. Further, the "Use of OPAR Datasets" policy defines additional procedures for managing access to data sets that include street address.
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?	Authorized individuals from the CFPB, Fannie Mae, Freddie Mac, Federal Reserve, HUD, and Census Bureau and other authorized users have access to NMDB data. These users are able to access NMDB data remotely by use of FHFA's externally facing Citrix environment. This requires multi-factor authentication and external users are restricted from transferring NMDB data outside of FHFA, they are only permitted to transfer the results of their analysis via FHFA's

#	Question	Response
		email system. The NMDB External User Access Control Procedures and NMDB Terms of Use address security and data governance.
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?	FHFA has mandatory annual IT Security and Privacy awareness training required of all employees and contractors, including external NMDB users.
6.4	Describe the technical/administrative safeguards in place to protect the data?	UNIX groups are utilized to control access to each dataset residing on MARS. Oracle security groups are used to control access to the Data Warehouse. Data owners approve all access to data sets under their control. Further, OPAR has developed a policy and specific procedures to minimize the extent to which actual street addresses are present and accessible in OPAR-controlled data files on the Analytics Platform. This includes running a program to mask street addresses in datasets, further restricting access to datasets that contain street addresses, and routinely reviewing users with access to data sets that contain street addresses.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Analytics Platform audit logs are delivered to FHFA's Security Information and Event Management (SIEM) solution and reviewed by FHFA's IT Security group.
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.	The Analytics Platform is in the continuous monitoring phase of the Risk Management Framework and undergoes annual security control assessments. The last SA&A was completed on September 11, 2018.
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 most recent ATO Memo for the FHFA Analytics Platform was signed on September 12, 2018.