



Privacy Impact Assessment Template

NATIONAL MORTGAGE DATABASE (NMDB)
(SYSTEM NAME)

November 6, 2013
DATE

This template is used when the Chief Privacy Officer 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 Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
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 information in identifiable form (“IIF”; also referred to Personally Identifiable Information (PII)) is handled. PIAs are to be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates IIF from or about members of the public; or 2) initiates a new electronic collection of IIF for 10 or more members of the public. PIAs are not required for collections of information from Federal employees. IIF about government personnel generally is protected by the Privacy Act; however the Office of Management and Budget (OMB) encourage agencies to conduct PIAs on these Systems, as appropriate. System Owners and Developers are responsible for completing the PIA.

The guidance below has been provided to help System Owners and Developers complete a PIA.

Overview

- In this section, provide a thorough 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 for 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.

FOR A PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- **Overview, Section 1, Section 2 & Section 6**

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 may 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 the Chief Privacy Officer.
- 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 the General Counsel Accountability Office or the FHFA 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 access 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 Certificate and Accreditation (C&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 C&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- According to OMB Circulars A-123 and A-130, 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. Describe these processes in response to this question.
- 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: 10/24/2013

System Name:			
NATIONAL MORTGAGE DATABASE (NMDB)			
System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Forrest Pafenberg	Forrest.pafenberg@fhfa.gov	NMDB	202 649 3129
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>NMDB is a comprehensive database of loan-level information about first lien single-family mortgages. In addition, for all individuals associated with a first lien single-family mortgage contained in the NMDB, the NMDB will also contain loan level information about all of those individual’s other credit lines, such as credit cards, student loans, auto loans, and other loans reported to credit bureaus. NMDB will be built from credit repository files: it is designed to be a nationally representative sample (5%) and the use of a sampling frame will permit the creation of a public use version of the database. This database will fulfill the monthly mortgage survey requirement of HERA.</p> <p>This will be a relational data set by merging HMDA, servicing data, Enterprise, and other government agency administrative data to capture loan-level data in five dimensions: mortgage record, real estate transaction, household demographic data on the borrower, physical characteristics of the house and neighborhood, and performance data on the mortgage and all credit lines (i.e. credit cards, student loans, auto loans, and other loans reported to credit bureaus) of the mortgage borrower and all those associated with the mortgage. The NMDB will be used to produce monthly performance data on mortgages credit lines. As part of this, data, which will become part of the NMDB, will be collected through a recurring National Survey of Mortgage Borrowers (NSMB).</p> <p>Beginning in 2014, a quarterly NSMB will collect mortgage search and satisfaction information from borrowers associated with newly sampled mortgages trade lines. The implementation strategy will be comprised of four planned contacts with potential respondents.</p>			

1. Week 1 Mail questionnaire and cover letter
2. Week 2 1st reminder letter
3. Week 5 2nd reminder letter plus questionnaire (only non-responders)
4. Week 7 3rd reminder letter (only non-responders)

A survey vendor will function as agent for the credit bureau (and FHFA), receiving returned mail and survey responses. By keeping track of who responded and non-delivered surveys, FHFA will be tracking individuals. The questionnaire ID number will allow the credit bureau (and its survey vendor) to merge survey data with NMDB mortgage trade lines (encrypted TINs). Individuals will have the opportunity to opt out of the survey by calling a survey hot line being maintained by the credit bureau or not responding at all. This number will be provided on the cover letter accompanying the survey questionnaire along with a Paperwork Reduction Act Notice and Privacy Act Notice.

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 collected, used, disseminated, or maintained in the System?	Data on a consumer’s mortgage, household composition, consumer housing characteristics, consumer performance on mortgages, and information about other credit lines such as credit cards, student loans, auto loans, and other loans reported to credit bureaus.
1.2	What are the sources of the information in the System?	Credit repository files, enterprise mortgage files, servicing files, property data files, HMDA, FHA, VA administrative data files, and survey results from individuals.
1.3	Why is the information being collected, used, disseminated, or maintained?	The NMDB will be a comprehensive dataset that can be used to regulate and monitor the housing and mortgage servicing sectors and to address a wide variety of economic and policy related topics. The information will be used to satisfy market report mandates as required under HERA for the FHFA or Dodd-Frank for the CFPB.
1.4	How is the information collected?	The information is collected from credit repository files, and servicing and property data files. Further, FHFA will collect data from FHA, HMDA, VA, and the Enterprises through interagency agreements and regulatory reporting. In addition, information will be collected directly from mortgage borrowers through the NSMB.

#	Question	Response
1.5	Given the amount and type of data collected, what risks to an individual’s privacy are associated with the data?	Risk of loss; identity theft; data integrity.

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	Describe the uses of information.	Mandatory reporting under HERA and Dodd-Frank, research, performance modeling, examination monitoring and other financial related analyses.
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.	Restricted access to data with mandatory non-disclosure agreements signed by those granted access; encrypted PIN and mortgage ID; redacted datasets for internal/external data use; third party intermediary to perform double blind merging of data.

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 information retained?	Permanent. Cutoff annually. Transfer data to NARA in 5 year blocks, in accordance with regulations in place at the time of transfer.
3.2	Has a retention schedule been approved by FHFA’s Records Management Officer and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes, N1-543-11-1 FHFA Comprehensive Records Schedule Item 2.3a Supervision and Housing Mission Electronic System Records.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Risk High immediately after received; risk (value) of dated information falls significantly over time.

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
---	----------	----------

#	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, FHFA -21 National Mortgage Database. It is in the process of being revised to reflect additional data fields that are being collected.
4.2	Was notice provided to the individual prior to collection of information?	For the survey, yes. In the cover letter to the survey questionnaire a Privacy Act Notice is provided to the individual.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes as it applies to the survey. As for other data sources, those are provided via a contract, Memoranda of Understanding (MOU), Interagency Agreements (IA), or required regulatory reporting.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals can direct requests for access to the Privacy Act Appeals Officer in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Individuals can direct requests to contest or appeal an adverse decision for a record to the Privacy Act Appeals Officer in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204.

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?	Internal use will be initially restricted to the FHFA NMDB team. Over time, data may be shared with other internal FHFA offices/divisions as needs arise.
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.	Eventually, CFPB, other federal government agencies, Fannie Mae, and Freddie Mac will have access to NMDB data. Data to be shared will include encrypted credit bureau trade lines to include mortgages, credit cards, student loans, auto loans, and other loans reported to credit bureaus and PINs, mortgage characteristics, property attributes, real estate transaction characteristics, and demographic information associated with sampled mortgage trade lines. A redacted public use dataset is envisioned in the future. Experian, performing double blind merging of data for NMDB, will be provided access to non-redacted mortgage, property,

#	Question	Response
		demographic, and real estate transaction data to facilitate high quality matching with credit bureau data.
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.	Yes. Yes. Sharing of PII with the credit bureau will be done for the purposes of high quality merging and matching of property data with credit bureau data.
5.4	Given the external sharing, explain the privacy risks identified (see question 1.5) and describe how they were/are mitigated.	Procedures are in place to limit access to CFPB staff and other federal government agency staff through MOUs/IAs. Risks are further mitigated through the use of encrypted PIN and mortgage ID; redacted datasets for internal/external data use; third party intermediary to perform double blind merging of data and signed non-disclosure agreements.

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? <u>If so, attach a copy to this PIA.</u>	System data and programs are located on FHFA's server. Currently, only FHFA Federal employees with access to the server and who are assigned to the NMDB restricted group can access the data and programs. The Project Lead or his designee requests access for team members via an email to the FHFA helpdesk. Access requests may also be generated via FHFA's internal access control system. Written procedures for access for FHFA employees assigned to this project are being developed.
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? <u>If so, attach a copy to this PIA.</u>	Yes. Selected Fannie Mae and Freddie Mac employees, CFPB employees and other government agency employees will have access to the system through VPN/Citrix security protocols. The Project Lead or his designee requests access for team members via an email to the FHFA helpdesk. Access requests may also be generated via FHFA's internal access control system.. Procedures for access by non-FHFA personnel assigned to this project are being developed.

#	Question	Response
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	FHFA policy requires any individual requiring access to FHFA's network (including any databases) to complete initial Rules of Behavior, and IT Security and Privacy Awareness training prior to being granted access to the network. In addition, authorized users are required to take this training on an annual basis after their initial access.
6.4	What technical safeguards are in place to protect the data?	Restricted access to data; two factor authentication; encrypted PIN and mortgage ID, and redacted datasets for internal/external data use.
6.5	What auditing measures are in place to protect the data?	NMDB will be part of the annual FHFA FISMA audit. Access control and auditing will be turned on. Project Lead will monitor user access on a regular basis and will file an annual audit of user access to the FHFA Chief Privacy Officer.
6.6	Has a Security Assessment and Authorization (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 C&A.	An SA&A has not been completed. However, one will be initiated in November 2013 and expected to be completed in January 2014.

Signatures

Forrest Peisenberg
 System Owner (Printed Name)

Forrest Peisenberg
 System Owner (Signature)

11/5/13
 Date

 System Developer (Printed Name)

 System Developer (Signature)

 Date

Ralph Mosios
 Chief Information Security Officer
 (Printed Name)

Ralph Mosios
 Chief Information Security Officer
 (Signature)

11/5/2013
 Date

[Signature]
 Chief Information Officer
 (Printed Name)

[Signature]
 Chief Information Officer
 (Signature)

11/5/2013
 Date

David A. Lyle
 Chief Privacy Officer
 (Printed Name)

[Signature]
 Chief Privacy Officer
 (Signature)

11/6/2013
 Date