



Privacy Impact Assessment Form
for
FHLBANK SYSTEM DIRECTORY

This document is only used when the Chief Privacy Officer determines that the system contains personally identifiable information and a more in depth assessment is required.

Complete and sign this form and forward to the Chief Privacy Officer.

David A. Lee
Federal Housing Finance Agency
1700 G Street NW
Washington, DC 20552
(202) 414-3804
David.Lee@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is handled. PIAs are to be completed when FHFA: 1) develops or procures IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or 2) initiates a new electronic collection of information in an identifiable form for 10 or more members of the public. System owners and developers are responsible for completing the assessment. The guidance below has been provided to help the system owners and developers complete the PIA.

Overview

- This section should provide a thorough and clear overview of the system and give the reader the appropriate context to understand the system owner's responses in the PIA. What is the purpose of the IT system? What will be the primary uses of the system? How will this support the 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 will 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, geographic, or financial, with no link to a name or other identifier, such as name, home address, social security number, account number, home telephone and fax numbers, or personal e-mail address.
- Examples of sources of the information include information that comes from individuals applying for loans, mortgages, and forms individuals completed. Where does the data originate? (e.g., the FHA, Office of Personnel Management, and Financial Institutions). 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, an organization).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB's approval to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act of 1980.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports the 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 a limited number of program staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires agencies to address the retention and disposal of information about individuals. (The retention information is published in the Privacy Act system of records notice).

- The retention periods of data/records that the agency manages are contained in either the NARA General Records Schedule or agency Records Schedule. For the data being created/maintained in the system, the records schedules are the authoritative sources for this information.
- 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 at 5 U.S.C. 552a(e)(1) 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."
- 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 personal identifier it is a Privacy Act system and may need a system of records notice (SORN) published in the Federal Register. The system may already have a Privacy Act SORN that applies to it. If you do not have a published SORN, contact the Privacy Act Officer. The Privacy Act requires that amendments to an existing system must also be addressed in a Federal Register notice. Any employee who knowingly and willfully maintains a systems 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.
- If a name or other personal 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 be protected from disclosure under the Freedom of Information Act.
- FHFA 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.
- The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

Section 5.0 Sharing and Disclosure

- If it is unknown to you whether or not systems share data, you can either contact the business owner of the data, or you can contact the IT specialist who knows what other interface goes on 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 GAO or the Inspector General. "Other" may also include database administrators or information system security officers. Also include organizations listed in the Privacy Act system of records

notice under the “Routine Use” section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.

- You must first review appropriate 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 statutory restrictions on use and disclosure of information that comes from a SORN.

Section 6.0 Technical Access and Security

- For the most part, access to data by a user within FHFA is determined by the “need-to-know” requirements of the Privacy Act (this means to authorized employees within the agency who have a need for the information to perform their duties). Care should be taken to ensure that only those employees who need the information have access to that information. Other considerations are the user’s profile based on the user’s job requirements and managerial decisions.
- The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?
- The system owner is responsible for ensuring that access to information and data is restricted to authorized personnel and by following the principle of least privilege. 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 to information needed to perform the user’s function in order to prevent user’s from having access to data or information not needed. 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.
- The IT Security Certification & Accreditation (C&A) process requires a system security plan that identifies the operational, technical, and management controls associated with identification and authentication of users. Certain laws and regulations require certain monitoring for authorized reasons by authorized employees. What is in place to ensure that only those authorized can monitor use of the system? For example, business rules, internal instructions, posting Privacy Warning Notices address access controls and violations for unauthorized monitoring and access. Business owners or managers of systems are responsible for preventing unauthorized monitoring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability is explicitly enabled or restricted. Business owners or managers of systems are responsible for preventing unauthorized access.
- The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. 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 some sort of control 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 in response to this question.
- Are there privacy and security awareness controls such as training materials for personnel? All employees, including contractors, have requirements for protecting information in Privacy Act systems
- Describe the controls in place to protect the information.

SUMMARY INFORMATION

Date submitted for review: March 29, 2011

Name of System: Federal Home Loan Bank System Directory (FHLBank System Directory)

System Owner(s): Division of FHLBank Regulation (DBR)

Name	E-mail	Phone #
Patricia L. Sweeney	pat.sweeney@fhfa.gov	(202) 408-2872

Overview

This section provides an overview of the system and addresses the following elements:

- 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 Overview

The primary purpose of the Directory is to provide and maintain current contact information on Federal Home Loan Bank Presidents, Chairs, Vice Chairs, Directors, Members of the Affordable Housing Advisory Councils (AHAC), and senior staff at the FHLBanks and the Office of Finance. This information is used in a business context and in support of the Division of FHLBank Regulation's (DBR) primary duty to ensure that the Federal Home Loan Banks (FHLBanks) operate safely and soundly. The DBR also assesses the FHLBanks' administration of their Affordable Housing and Community Investment Programs (AHP and CIP, respectively).

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, rule, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of personally identifiable information (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?	The Directory contains information normally found in a phone or directory listing such as: name, phone number, e-mail, company, title, address, and as appropriate, terms of office for members of an FHLBank's Board of Directors.
1.2	What are the sources of the information in the system?	The FHLBank system administrators enter the relevant data for their FHLBank. The FHFA system administrators have the authority to modify or correct the data, as needed.
1.3	Why is the information being collected, used, disseminated, or maintained?	The primary purpose of the Directory is to provide and maintain current contact information on FHLB Presidents, Chairs, Vice Chairs, Directors, Members of the AHACs, and senior staff at the FHLBanks and Office of Finance.
1.4	How is the information collected?	Manual data entry from FHLBank Administrators.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Minimal risk as this information is primarily business related. However, it is possible that some data may include a home address as some Directors have home-based businesses, or are retired.

Section 2.0 Uses of the Information

The following questions clearly delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	Describe the uses of information.	The DBR admin staff uses Directory data for administrative purposes in preparation for and during the various phases of the FHLBank examination process. For internal FHFA use, FHLBank addresses are also provided for ministerial functions such as FHLBank assessments.

#	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.	Access to Directory data is limited to authorized users. All users must be members of the FHFA's domain. Each user is placed in the appropriate Active Directory group. Further controls are in place to determine the specific permission, such as read only, or read/write. The FHLBank system administrators are the single authority in making the determination on access and permission level at their FHLBank. Presently, while access is restricted to each individual FHLBank's data, FHFA employees do not have this restriction. The data entry point for the Directory is the FHFA's domain, i.e., https://extranet.fhfa.gov / FHFA Applications / FHLBank System Directory. Each approved user has a unique username and password which is issued by the FHFA in accordance with procedures, which in turn, prevents unknown or unregistered IP addresses to access the Directory.

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?	The Directory data is refreshed on an annual basis. There is no archiving function.
3.2	Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?	Does not apply. There is no archiving function. The Directory data is real-time and refreshed on an annual basis, at a minimum.
3.3	Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Does not apply. See responses 3.1 and 3.2.

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?	Yes – FHFA-8
4.2	Was notice provided to the individual prior to collection of information?	Yes. This is done via the access request form and lead into the extranet.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes. This is not a mandatory system. Also, the system administrators at the FHLBanks are responsible for entering the Directory data for the FHLBank.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may request a copy of their information from their system administrator.
4.5	What are the procedures for correcting inaccurate or erroneous information?	The system administrator at each FHLBank is responsible for maintaining and updating the information. This person is responsible for ensuring accurate data entry, and in the event of error, is also responsible for correcting the information.

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?	Staff in DBR and authorized users at the FHLBanks have access to the Directory data, the scope of which is limited to what is minimally necessary and pertinent to meet the single purpose of the Directory – to provide and maintain current contact information for internal access/ use only.

#	Question	Response
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 Directory data is not shared with Federal, state or local government, or the private sector. (See response to 5.1 above.)
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? If so, please describe. If not, please describe under what legal authority the program or system is allowed to share the PII outside of the agency.	This question does not apply, as Directory access is restricted to authorized users and the Directory data is not shared outside the agency, as reflected in responses 5.1 and 5.2 above.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Directory access is restricted to authorized users and the Directory data is not shared outside the agency. See responses 5.1 and 5.2.

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 and are these procedures documented?	System access is based on being members of the FHFA's domain; being placed in the correct Active Directory groups; and being added to the system itself. Further controls are in place to determine if an individual will have the ability to read only, or to actually add/modify data.
6.2	Will contractors have access to the system? If yes, how will contractors gain access to the system? How will the agency control their access and use of information?	FHFA IT contractors would be the only possible contractors who could have access to the system. Presently, no IT-related work on the Directory is in progress, nor is any IT-related work scheduled to be done.

FHFA PIA FOR: FHLBank System Directory
(System Name)

#	Question	Response
6.3	Describe what privacy training is provided to users either generally or specifically relevant to the program or system?	DBR staff complete annual privacy awareness training.
6.4	What technical safeguards are in place to protect the data?	The data is encrypted and stored in an SQL repository with restricted access.
6.5	What auditing measures are in place to protect the data?	The Directory is fully audited. Every access, update, addition, report and process is audited.
6.6	Has a Certification & Accreditation been completed for the system?	Certification & Accreditation is not required for this system.

Patricia L. Sweeney
System Owner (Printed Name)


System Owner (Signature)

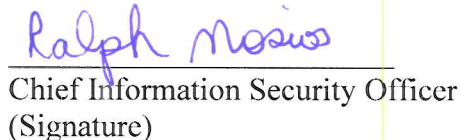
4/5/2011
Date

Anthony Vitale
System Developer (Printed Name)


System Developer (Signature)

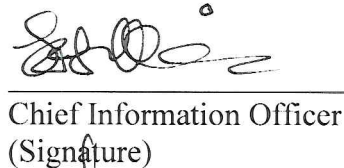
4/5/2011
Date

Ralph H. Mosios
Chief Information Security Officer
(Printed Name)


Chief Information Security Officer
(Signature)

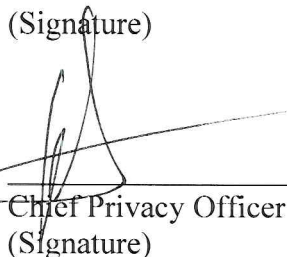
4/7/2011
Date

Kevin Winkler
Chief Information Officer
(Printed Name)


Chief Information Officer
(Signature)

4/7/11
Date

David A. Lee
Chief Privacy Officer
(Printed Name)


Chief Privacy Officer
(Signature)

4/7/2011
Date