Privacy Impact Assessment Form

LITIGATION SUPPORT SYSTEM
(SYSTEM NAME)

This template is 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 template and forward to the Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
Senior Agency Official for Privacy
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. 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 OM B's approval to do so or determine whether OM B'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)(l) 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.
- 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.
- 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 IT 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. 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 may 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.
- The IT Security 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 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. It is the responsibility of managers of systems to ensure 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 is explicitly enabled or restricted. It is the responsibility of managers of systems to ensure no unauthorized access is occurring.
- 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 OM B 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: 9/17/10

Name of System: **Litigation Support System (LSS)**

System Owner(s):

Name	E-mail	Phone#
Kathleen K. berg	Kathleen.Berg@fhfa.gov	202-3431817

Overview

The overview section provides an overview of the system and should address 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 system name is the Litigation Support System that is owned by the Office of Governance (OG). The database was created to host the Fannie Mae Special Examination documentation. It supports the agency function to examine the safety and soundness of the enterprises and conduct research associated with litigation.

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 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?	A small percentage of personal or sensitive information may have been inadvertently collected such as name, income, educational level, employment history with possibly a social security number, date of birth, or home/personal email address or phone number. The type of information is accounting, auditing, corporate governance, compensation, internal controls and political activity information was requested from Fannie Mae, Fannie Mae independent counsel, or outside accountants, in order to review certain issues of the Enterprise.
1.2	What are the sources of the information in the system?	The sources of information were provided by Fannie Mae; the Enterprise's accountants, KPMG and Ernst & Young LLP; or by the Enterprise's independent legal counsel, Paul Weiss LLP. The electronic information sent in CDs is stored in locked container.
1.3	Why is the information being collected, used, disseminated, or maintained?	Data was primarily requested by subpoena for the investigation of accounting issues of the Enterprise. The examination ended in 2006, and no further data was subsequently collected. It is being maintained to respond to FOIA requests, or conduct research associated with litigation.
1.4	How is the information collected?	The overwhelming majority of data was collected from and reviewed by the individuals and by the Enterprise, or by the Enterprise outside accountants, or by the Enterprise's independent counsel, who then submitted it to OFHEO/FHFA. A few individuals submitted personal and financial information to OFHEO/FHFA through their counsel prior to being interviewed by the agency. This information may have included

#	Question	Response
		employment, professional or compensation information.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The general intent of collection was not to collect personal information; however, it may contain but not disseminate a small percentage of personal or sensitive information may have been inadvertently collected such as name, income, educational level, employment history with possibly a social security number, date of birth, or home/personal email address or phone number.

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.	The information was collected in response to the 2006 Fannie Mac Special Examination and currently serves as the official record of the collection for research.
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 LSS IS approved by OGC/OG for specific use; login password and permissions restrict access; and permissions protect modification.

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?	Data is retained for 15 years after the Administrative Hearing or Litigation is closed in accordance with FHFA's Records Retention Schedule

#	Question	Response
3.2	Has a retention schedule been approved by the Agency's Records Management Officer and NARA? If yes, provide the corresponding GRS or Agency specific Records Schedule number.	Yes, the schedule was submitted by the records officer to NARA. The schedule was approved by Archivist of the U.S. on 9/18/09. The retention schedule job number is N 1-543-09-1.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Time-related risks include the corruption, loss, or change of electronic data. The General Support System (GSS) for the agency maintains the LSS and performs a daily backup to recover data changes or data loss; In addition, the agency emergency disaster COOP hot site facility replicates in real time LSS data, and is part of the GSS operating under IT security policy and procedures.

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.	Yes, it is part of the Litigation Enforcement Information System (LEIS).
4.2	Was notice provided to the individual prior to collection of information?	Notice would have been provided the Enterprise counsel prior to sending it to FHFA.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	The information was required by subpoena therefore it was required by law enforcement act. That opportunity was determined by the Enterprise counsel prior to sending it to FHFA.
4.4	What are the procedures that allow individuals to gain access to their information?	The individual or their attorney would contact the Enterprise counsel.

#	Question	Response
4.5	What are the procedures for correcting inaccurate or erroneous information	Enterprise counsel would notify and deliver to the agency any correction of inaccurate or erroneous information, which would be changed and documented in the LSS Media Log, an excel spreadsheet in the daily backup system of the GSS.

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?	Individuals within the Offices of General Counsel, Division of Enterprise Regulation, and Technology and Information Management have access to support legal research, FOIA, and database management.
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.	By law, the special examination documents could be shared with another federal agency, such as the IRS, DOJ for matters under investigation.
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, describe. If not, describe under what legal authority the program or system is allowed to share PII outside of the agency.	Sharing of the special examination documentation PII is covered under the LEIS SORN.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Privacy risk identification and mitigation are handled through FHFA Office of General of Counsel under FHFA regulations and federal privacy laws.

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? If so, attach a copy to this PIA.	In response to OGC/OG request, access to LSS is controlled through OTIM Systems Engineer through login, password control access and permission protections procedures that are documented under the Server Security Lockdown Procedures in the disaster recovery plan for Litigation Support Server.
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? Are there procedures documented in writing? If so, attach a copy to this PIA.	OGC & OG determine when and which contractors need access to LSS; and OTIM Systems Engineer controls access and use of information through login, password control access and permission protections.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	Agency privacy training is required for all employees, including contractors, on an annual basis. Contractors must sign a non-disclosure agreement.
6.4	What technical safeguards are in place to protect the data?	Database access requires individual login and unique password; permission protection controls data modification and users have limited ""read only" access to LSS.
6.5	What auditing measures are in place to protect the data?	No changes can be made to the core collection by users. The LSS database 1s a static repository, receives no new documentation nor has any business requirement; it is part of the daily backup to recover data changes or data loss under the General Support System for the agency.
6.6	Has a C&A been completed for the system or systems supporting the program? If so, provide the date the last C&A was completed.	Yes, currently expired due to the system being retired.

Signature Page

Kathleen K. Berg
System Owner (Printed Name)

Kathleen Berg
System Owner (Signature)

11/10/10
10/01/10
Date

n/a
System Developer (Printed Name)

n/a
System Developer (Signature)

Date

Jeffrey T. Test, Ph.D.
Chief Information Security Officer
(Printed Name)

Jeffrey T Test
Chief Information Security Officer
(Signature)

Oct 13, 2010
Date

Robert Kevin Winkler
Chief Information Officer
(Printed Name)

Chief Information Officer
(Signature)

10/26/2010
Date

David A. Lee
Chief Privacy Officer
(Printed Name)

Chief Privacy Officer
(Signature)

11/10/2010
Date