



Privacy Impact Assessment Template

TRAINING REQUESTS APPLICATION

JANUARY 8, 2016

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 as 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) encourages 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
- Sections 1, 2, and 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 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.
- 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: _____

System Name:			
System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Dave Freimuth	David.freimuth@fhfa.gov	OHRM/LA	202-649-3481
Bob Stanton	Robert.stanton@fhfa.gov	OHRM/LA	202-649-3750
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 Training Request application automates the (Standard Form) SF-182 form and the related justification (FHFA Form #037) allowing FHFA staff to request external training. The system provides for the creation, review, approval, and archiving of training requests and will produce reports summarizing training and expenses.			

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?	All information collected on the standard SF-182 form including name, business address and telephone number, email address, and employment status, pay plan, series, and grade. Also, information about the requested training event and estimated costs.

#	Question	Response
1.2	What are the sources of the information in the System?	Information about the training event is input by the person requesting training. Information about employment status, etc. is automatically uploaded from employment records.
1.3	Why is the information being collected, used, disseminated, or maintained?	Provides a system to apply for the application/justification, review, approval, archive, and report external training requests.
1.4	How is the information collected?	Information about the training event is input by the requester.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	There is minimal risk if data in the system were be compromised or accessed by an unauthorized user as the data consists only of employee agency contact information, pay grade, and training information.

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 is used to track approved external training events.
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.	Administrator access to the Training Requests Application is limited to training and budget approvers who have been authorized by a system owner. Data within the application consists only of information contained within the Training Request Form (SF 182) which includes details about the training course, and the Training Justification Form (Form 037) which explains the purpose and benefit of the training. This data can be printed as completed versions of the SF 182 and Form 037, however, this action would appear as an event in the application audit log which is reviewed by the system owner each week.

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?	n/a
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.	n/a
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	n/a

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.	n/a
4.2	Was notice provided to the individual prior to collection of information?	n/a
4.3	Do individuals have the opportunity and/or right to decline to provide information?	n/a
4.4	What are the procedures that allow individuals to gain access to their information?	n/a
4.5	What are the procedures for correcting inaccurate or erroneous information?	n/a

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?	n/a
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.	n/a
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
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	n/a

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>	Training Request Access Control and Audit Procedures have been developed which describe the privileges associated with each system role, and procedures for authorizing users with privileged accounts.
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>	No non-FHFA personnel will have access.

FHFA PIA FOR: Training Requests Application

#	Question	Response
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	Training is being developed and will be available in early 2016.
6.4	What technical safeguards are in place to protect the data?	Application access is restricted through active directory security groups. Users must be assigned to a specific active directory security group in order to gain access to the application. Further, privileged access is restricted to only authorized system administrators. All user activity is audited.
6.5	What auditing measures are in place to protect the data?	All system activity is audited and reviewed weekly by system owners (including the system administrator) as described in the Access Control and Audit Procedures.
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 application was characterized as Non-FISMA Reportable and was not subject to a full SA&A, however, Access Control and Audit Procedures have been established and are being carried out by system owners.

Signatures

David Freimuth
System Owner (Printed Name)

David Freimuth
System Owner (Signature)

1/3/2016
Date

Brad Blackmon
System Developer (Printed Name)

Brad Blackmon
System Developer (Signature)

1/4/2016
Date

Ralph Mosios
Chief Information Security Officer
(Printed Name)

Ralph Mosios
Chief Information Security Officer
(Signature)

1/7/2016
Date

Kevin Winkler
Chief Information Officer
(Printed Name)

Kevin Winkler
Chief Information Officer
(Signature)

1/8/2016
Date

David A. Lee
Chief Privacy Officer
(Printed Name)

David A. Lee
Chief Privacy Officer
(Signature)

1/8/2016
Date



Federal Housing Finance Agency
Access Control and Audit Procedures
For
Training Request System
Release Date: November 25, 2015

Approval: David A. Freimuth 12/2/2015
Training Request System Owner Date

1. Introduction

The Training Request System allows FHFA employees to electronically complete two forms required to request external training. The two forms are:

1. Training Request Form SF182: *Authorization, Agreement and Certification of Training* and,
2. FHFA Form #037: *Training Justification*.

Users enter information related to their requested external training courses, such as date, location vendor, cost, etc. and submit for approval. Training request require approval from, at minimum, the user’s supervisor and a Training Request administrator.

For each training event that has received approval, employees are required to certify that the training was attended and completed. After the end date of a scheduled training event passes, users are required to access the Training Request system and certify that they have attended and completed the event.

2. Training Request System Owners

Role	Name	Phone	Email
System Owner	David Freimuth	202-649-3481	David.freimuth@fhfa.gov
System Owner	Bob Stanton	202-649-3750	Robert.stanton@fhfa.gov

Figure 1: Training Request System Owners

3.4. Account Management

At least annually, OTIM Security shall generate the list of current Training Request privileged users and their assigned roles, and will provide the list to the Training Request System Owners to review and determine if all users still need access to the system or if any accounts can be removed or permission levels reduced in accordance with the principle of least privilege.

The System Owner will mark any changes in access on the printed copy of the user list, and will sign and date a user authorization form provided by OTIM Security. The results will be made available to OTIM Security for record. Changes will be submitted to Help Desk by the System Owner.

4. Audit Log Review Process

Every Monday, an audit report is generated from Audit Central that records all user activity that occurred in the Training Request System within the prior 7 days. This report is delivered as a .pdf file via email to the Training Request system owner at 8:00am EST.

The system owner reviews the log for unusual or suspicious activity, and at the completion of the review, replies via email to #AuditLogReview indicating that the log has been reviewed, and whether or not any unusual activity was observed.

5. Document Maintenance

The Training Request system owner will be responsible for updating this procedure whenever changes occur.