



**Privacy Impact Assessment Template**

**VISITOR MANAGEMENT SYSTEM**  
**(SYSTEM NAME)**

7/5/2016

**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 7<sup>th</sup> Street SW  
Washington, DC 20024  
(202) 649-3803  
[Privacy@fhfa.gov](mailto: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) 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

## FHFA PIA FOR VISITOR MANAGEMENT SYSTEM

Page 3 of 11

- 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:** \_\_\_\_\_

<b>System Name: Visitor Management System</b>			
<b>System Owner(s)</b>			
<b>Name</b>	<b>E-mail</b>	<b>Division/Office</b>	<b>Office Phone Number</b>
Katrina Jones	katrina.jones@fhfa.gov	OFOM	202-649-3789
<b>System Overview:</b> 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>The Visitor Management System falls under the Office of the Chief Operating Officer in the area of Access Control. The Visitor Management System allows for the automation of the currently utilized paper based Visitor Management System. The new system will utilize an application housed on FHFA's network to generate a visitor request form. This form will be emailed to the FHFA Emergency email address where it will be printed out on a daily basis and hand carried to each of the guard desks located at 400 7th Street NW for use by the guards when admitting visitors to FHFA space</p>			

**FHFA PIA FOR VISITOR MANAGEMENT SYSTEM**

**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?	Visitor Name Visitor Organization FHFA POC Name FHFA POC contact number office and cell Date and Time of the meeting FHFA Destination Visiting Type (Business Visit or Personal Visit) Comments (free form text)
1.2	What are the sources of the information in the System?	The information comes from two sources. Work information (i.e., FHFA-issued e-mail address, office desk telephone number and iPhone/ BB telephone number) and Visitor via the FHFA POC.
1.3	Why is the information being collected, used, disseminated, or maintained?	The primary purposes are to contact employees and contractors to let them know that their visitor is in the building. Constitution Center is a privately owned building and all persons entering the building must have badge access or be escorted by someone with badge access. Only persons on the daily visitor list are allowed to begin the security clearance process.
1.4	How is the information collected?	FHFA information is provided by the FHFA host or their designee. The FHFA host also provides the name of the visitor and the date and time of the visit.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	In the event of a data loss or mishandled data, the risk to personal privacy of FHFA personnel is that their personal information, specifically their name and work phone numbers (desk and iPhone/BB) have the potential of being compromised. The visitor's name has the potential of being compromised.

**Section 2.0 Uses of the Information**

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

**FHFA PIA FOR VISITOR MANAGEMENT SYSTEM**

#	Question	Response
2.1	Describe the uses of information.	To verify and coordinate access for visitors to FHFA spaces.
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.	Only authorized users will have access to the information, specifically the System Owner, the FHFA host, Constitution Center guard services personnel, and authorized OTIM IT Security personnel. Authorized administrators will have the ability to run reports, and monitor the user and data being requested and grant and remove user accounts and permissions. OTIM IT Security will further have the ability to check/track log files, system penetrations and misuse of the system.

**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?	Information is destroyed 7 years after cutoff. Cutoff occurs when the project/activity /transaction is completed or superseded.
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. Records are scheduled in FHFA's Comprehensive Records Schedule as Item 5.1 – Administrative Management Records. The NARA Authority for this records schedule is N1-543-11-1.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	All data is stored within VMS. Because the system has been developed and is hosted by FHFA, this will decrease the risk of data loss due to hacking or nefarious means. All data will be stored to meet FHFA OTIM security and the National Archives record guidelines, and will be stored and secured by OTIM until the data meets the record retention end date. At that time OTIM will sanitize the data to NIST 800-88 guidelines.

**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.

**FHFA PIA FOR VISITOR MANAGEMENT SYSTEM**

#	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-17 - Visitor Badge, Employee and Contractor Personnel Day Pass, and Trackable Mail System.
4.2	Was notice provided to the individual prior to collection of information?	Notice is not provided as employee work information is collected from FHFA Systems, and for visitors information is collected by the FHFA POC.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes, however access to the building will be denied.
4.4	What are the procedures that allow individuals to gain access to their information?	Not applicable. Individuals visiting FHFA will not have access to the data system.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Inaccurate or erroneous information can be corrected by the system administrator, system owner or the user (FHFA POC) correcting the information that they had inputted.

**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?	The information gathered will be available to OTIM, the System Owner, and other authorized FHFA employees. It will be shared with OTIM, IT Security Unit since they have responsibility for safeguarding all FHFA information technology, protecting information systems and ensuring confidentiality, integrity, and availability of IT resources.
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.	Information is shared with Constitution Center security guards so that they can confirm visitor's appointment via VMS, complete the check-in process and print visitor's badges. There exists the possibility that outside agencies (e.g., DoJ/FBI; DHS/FEMA; courts; magistrates; members of advisory committees that are created by FHFA or by Congress;

**FHFA PIA FOR VISITOR MANAGEMENT SYSTEM**

#	Question	Response
		members of Congress; and other performing or working on a contract; officials of a labor organization; Office of Management and Budget; and the Office of the Inspector General), may request access to stored data for investigational purposes or to any federal government authority for the purpose of coordinating and reviewing agency continuity of operations plans or emergency contingency plans developed for responding to Department of Homeland Security threat alerts, weather related emergencies, or other critical situations.
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
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	The primary risk is that an user (FHFA POC) or visitor will have their inputted data exposed should the information be lost or otherwise compromised. FHFA OTIM IT Security has established procedures for securely managing access to the application and for reviewing user activity for indications of inappropriate use.

**Section 6.0 Technical Access and Security**

The following questions describe technical safeguards and security measures.

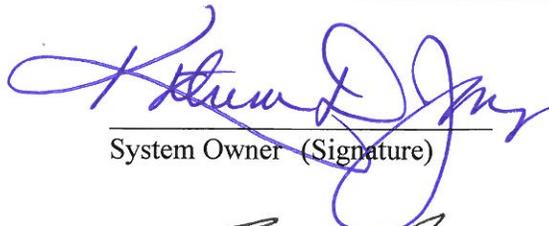
#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? <u>If so, attach a copy to this PIA.</u>	All FHFA users will have access to VMS as a user. Only limited personnel authorized by the system owner will be granted Administrator access. The VMS system security plan (SSP) defines the account management procedures.
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>	All FHFA users (employees and contractors) will have user-level access to VMS, in order to submit new visitors. VMS is not accessible by Non-FHFA personnel.

**FHFA PIA FOR VISITOR MANAGEMENT SYSTEM**

#	Question	Response
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	All FHFA employees are required to participate in annual Information System Security Awareness and Privacy Training. Further, privileged FHFA users are trained on account management procedures and audit log review procedures by OTIM Security
6.4	What technical safeguards are in place to protect the data?	Application access is restricted through active directory security groups as well as application accounts. All users must have an active FHFA Active Directory account and be a member of the appropriate security group in order to access the application. Administrators must have an active FHFA Active Directory account, and must also be granted an application account within VMS.
6.5	What auditing measures are in place to protect the data?	OTIM has developed an automated audit log report that indicates all changes in user-roles within VMS, such as the addition of new users, or changes to permissions for existing users. OFOM reviews these audit log reports to ensure that all changes to users and permission levels have been approved.
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.	VMS has undergone a full SA&A and the Authorization to Operation (ATO) is expected to be signed in June 2016.

**Signatures**

KATRINA D. JONES  
System Owner (Printed Name)

  
System Owner (Signature)

7/5/16  
Date

BRIAN BLACKMON  
System Developer (Printed Name)

  
System Developer (Signature)

7/7/16  
Date

Ralph Mosios  
Chief Information Security Officer  
(Printed Name)

Ralph Mosios  
Chief Information Security Officer  
(Signature)

7/7/2016  
Date

FHFA PIA FOR VISITOR MANAGEMENT SYSTEM



Chief Information Officer  
(Printed Name)

P. Kent Winkler

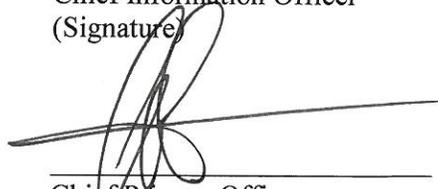
Chief Information Officer  
(Signature)

Page 11 of 11

7/7/2016  
Date



Chief Privacy Officer  
(Printed Name)



Chief Privacy Officer  
(Signature)

7/7/2016  
Date