
**Privacy Impact Assessment (PIA) Template**

**VISITOR MANAGEMENT SYSTEM**
**(Name of the Information System or Information Collection)**

**January 2024**
**Date**

| System/Collection Overview |
|---|
| The Visitor Management System (VMS) is an internally developed application housed on FHFA's network and managed by the Office of the Chief Operating Officer. VMS is the automation of the previously utilized paper-based Visitor Management System and is designed to generate a request for visitor access. Security personnel or designated representatives within the Office of Facilities Operations Management (OFOM) then use this information to consolidate and email a list of daily visitors to Constitution Center's (CC) Security Operations Center (SOC). SOC security personnel subsequently email a copy of the daily visitor lists to each security guard desk located at 400 7th Street SW, Washington, DC for use by the security guards when admitting visitors to CC and FHFA spaces. |

**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 System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

| # | Question | Response |
|---|---|---|
| 1.1 | What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection? | The system collects the visitor's name and organization, FHFA point of contact (POC)/sponsor or designee name, office and/or cell number, date and time of the visit, FHFA destination, visit type (business or personal visit), and comments (via free form text). |
| 1.2 | What or who are the sources of the information provided to FHFA and included in the System/Collection? | The information comes from two sources: the Active Directory and FHFA POC/sponsor or their designee. The FHFA employee's work information (i.e., FHFA-issued e-mail address, office desk telephone number and iPhone number) is auto-generated from the Active Directory when the employee logs in and provides the visitor information. |

| | | |
|---|---|---|
| 1.3 | For what purpose is the information being collected, used, disseminated, or maintained? | The primary purpose is to maintain accountability of FHFA visitors entering CC and FHFA spaces. CC is a privately owned building and all persons entering the building must have badge access or be escorted by someone with badge access. Personnel without badge access to CC or FHFA spaces must be entered into the VMS prior to receiving security screening from CC security guards. Once the visitor completes security screening, the visitor list is used to identify and contact the FHFA POC/sponsor or designee to let them know their visitor is in the building. |
| 1.4 | How is the information provided to or otherwise obtained by the System/Collection? | Information is prepopulated into the system via the Active Directory and provided by the FHFA POC/sponsor or their designee. |
| 1.5 | Are Social Security Numbers (SSNs) being collected or used in the System/Collection?<br>• If yes, describe in detail:<br>1) The business justification for collecting or using SSNs;<br>2) The consequences if SSNs are not collected or used; and<br>3) How the SSNs will be protected while in use, in transit and in storage.<br>• If no, state "N/A" in the response section. | N/A. SSNs are not collected or used in the system. |

**Section 2.0 Uses of the Information**

The following questions delineate the use of information.

| # | Question | Response |
|---|---|---|
| 2.1 | How will the information be used and for what purpose? | The information will be used to verify and coordinate access for visitors to CC and FHFA spaces. |
| 2.2 | Describe any types of measures or processes 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 POC/sponsor, OFOM designated personnel, Constitution Center security guard services personnel, and authorized Office of Technology and Information Management (OTIM) Information Technology (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 the information retained? | Information is destroyed seven (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 Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (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. |

**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 the individual's ability to ensure the accuracy of the information collected about them.

| # | Question | Response |
|---|---|---|
| 4.1 | Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification?<br>• If no, please put "no" in the Response section.<br>• If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress. | Yes. SORN FHFA-17 - Visitor Badge, Employee and Contractor Personnel Day Pass, and Trackable Mail System applies to this system. |
| 4.2 | How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not. | Notice is not provided because this system is not the original point of collection. Employee work information is collected from the Active Directory, and visitors' information is collected by the FHFA POC/sponsor or designee. |
| 4.3 | Is an individual's response to the request for information voluntary or mandatory? | Voluntary. |
| 4.4 | What are the consequences if an individual declines to provide the information? | Access to the building will be denied if an individual declines to provide the information. |
| 4.5 | What are the procedures that allow individuals to gain access to their information? | Individuals can direct requests for access to the Privacy Office in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204. |

| | | |
|---|---|---|
| 4.6 | 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/sponsor) correcting the information that they inputted. Individuals can also direct requests to correct or amend their contact information to the Privacy Office in accordance with the SORN and FHFA's Privacy Act Regulation, 12 CFR 1204. Additionally, individuals can direct requests to contest or appeal an adverse decision for a requested correction or amendment to 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 | Is information shared with internal office(s) or division(s)?<br>• If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose.<br>• If no, please state "N/A" in the response section. | The information gathered will be available to OTIM and other authorized FHFA employees on a need-to-know basis. |
| 5.2 | Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector.<br>• If yes, please identify the information shared, and for what purpose.<br>• If no, skip to Section 6. | Information is shared with CC security guards so they can confirm visitor appointments via VMS, complete the security screening and check-in process, and print visitor badges. There exists the possibility that outside agencies (e.g., Department of Justice (DOJ)/Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA), courts, magistrates, members of advisory committees that are created by FHFA or Congress, members of Congress and others performing or working on a contract, officials of a labor organization, Office of Management and Budget (OMB), and the Office of the Inspector General (OIG)) may request access to stored data for investigation 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 DHS threat alerts, weather related emergencies, or other critical situations. |

| | | |
|---|---|---|
| 5.3 | Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection?<br>• If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1.<br>• If no and/or a SORN a does not apply, identify the legal authority that permits the sharing outside FHFA. | Yes. See routine uses for SORN, FHFA-17. |

**Section 6.0 Technical Access and Security**

The following questions describe technical safeguards and security measures.

| # | Question | Response |
|---|---|---|
| 6.1 | Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein?<br>• If yes, how will they gain access to the System/Collection?<br>• If no, how will the agency control access to and use of that information?<br>• Are there procedures or criteria documented in writing? If so, please describe. | VMS is not accessible by FHFA OIG or non-FHFA personnel.<br><br>All FHFA users (employees and contractors) will have user-level access to VMS in order to submit new visitors. 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 | Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed. | No. |
| 6.3 | Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection. | A user manual is available to all FHFA users that describes the basic instructions for the use of VMS. |
| 6.4 | Describe the technical/administrative safeguards in place to protect the data. | The system is only accessible to FHFA employees and contractors with internal network accounts. Users can only view requests for visitors they have submitted themselves.<br><br>All application activity is audited, and available to system administrators as needed. |

**Section 7.0 Risk**

The following questions describe the risk to the information within the System or Collection.

| # | Question | Response |
|---|---|---|
| 7.1 | Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated. | In the event of a data loss or mishandled data, the risk to personal privacy of FHFA personnel is that their business information, specifically their name and work phone numbers (desk and iPhone) have the potential of being compromised. The visitor's name also has the potential of being 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. |
| 7.2 | 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 other nefarious means. All data will be stored to meet FHFA OTIM security and the National Archives and Records Administration (NARA) 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. |
| 7.3 | Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated. | The primary risk is that a user (FHFA POC/sponsor or designee) 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. |