Privacy Impact Assessment Template

FM: SYSTEMS
(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 **(IIF)** 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 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 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.

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 an organization such as Mortgage Bankers).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB prior approval 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 the Agency's or 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 of 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, the 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)(l).
- 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 (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 Privacy Act Officer. The Privacy Act requires that any amendments to an existing system must also be addressed in a Federal Register notice.
- 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 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 (l2 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 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.

Section 5.0 Sharing and Disclosure

- If it is unknown 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 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 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 Technical Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The IT Security Certificate and Accreditation (C&A) process requires a system security plan that identifies the technical controls associated with identification and authentication of users. Certain Jaws 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 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 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:

Name of System:

System Owner(s) (including Division/Office):

Name	E-mail	Phone#
Daniel Berkland	Dan.berkland@fhfa.gov	202-408-2902
Dave Gilson	Dave.gilson@fhfa.gov	202-414-3105
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 Office of the Deputy Chief Operating Officer has purchased facility management software (FM Systems) to assist in coordinating the move of FHFA personnel and assets move to Constitution Center, the agency's new headquarters facility. The system will be used to assign office spaces to employees and contractors to support space planning activities assigned to the Facility Management Office (FMO) as well as for asset management and moves after occupying the new space.		

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?	For all employees and contractors of the Agency the system will include FHFA employees and contract personnel as listed in the agency active directory, office telephone number, office email address, office/room number, assets issued to the individual (i.e. telephone, laptop, desktop printer), and division and office name.

#	Question	Response
1.2	What are the sources of the information in the system?	Design floor plans developed by the agency hired A-E firm, Studios Architecture; name and telephone and office information from the Active Directory and the remaining information regarding IT items assigned and placed in offices will be entered manually by facility staff.
1.3	Why is the information being collected, used, disseminated, or maintained?	To facilitate the move of all Agency personnel from three current locations into one building. After the move the information will be used to manage FHFA assets.
1.4	How is the information collected?	Initial data population will be from A-E AutoCADD digital floor plans. The remainder will be entered manually (names and telephone numbers). If the capability exists, division and office affiliation will be entered through an automatic update from FHFA's active directory to FM Systems software. After initial deployment, the intent will be to have either active directory auto populate information obtained from FMO when a new employee enters the agency, or through manual entry by FMO.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The risk to an individual's privacy is low because there is no PII information (other than name) being housed in the system.

Section 2.0 Uses of the Information

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

#	Question	Response
2.1	Describe the uses of information.	Arrange the seating locations for FHFA's employees and contractors. Set up multiple scenarios for FHFA to consider when making these decisions.
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.	The controls start at the firewall where access to the client's VM is isolated to client specified points of egress. Only required ports are opened to those points. An optional component is a VPN tunnel from each client site. All connections are encrypted via SSL Certificates. Next is that all client data is stored in client specific databases that are secured such that they can only be

#	Question	Response
		accessed by the client's logins (FM Support and FM Systems Hosting departments and the FM Systems Consultant assigned to the project also have access). Per FM Systems Employee Handbook and the Hosting Acceptable Use Policy, all data is treated as confidential. As such, all backups and data transfers are encrypted, per policy.

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	Backup files for contracts that have been terminated will be deleted from both the Primary and DR servers within 45 days of the contract terminating. A backup of each of the production SQL database and SSRS RDL files shall be provided to the client in an encrypted ZIP file upon termination of the contract. A note shall be entered into the hosting tracking system that the backup jobs have been deleted, the VM has been deleted and the VHDs removed, that the backup files are marked for deletion, that all SQL databases have been deleted, and who did each task. Within 30 days, there shall be an additional entry that shows who verified that the deletions were successful from all systems with the date of verification. The official records managed and retained by FHFA facility staff will be In Accordance With (IAW) FHFA's Comprehensive Records Schedule, which is to destroy the records seven years after cutoff.
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.	Records related to property accountability, building security, emergency planning, space planning and maintenance, property disposal, motor vehicle maintenance and operations, and mail and courier services, and other administrative support services.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	All client data is stored in client specific databases that are secured such that they can only be accessed by the client's logins (FM Support and FM Systems Hosting departments and the FM Systems Consultant assigned to the project

#	Question	Response
		also have access). Per FM Systems Employee Handbook and the Hosting Acceptable Use Policy, all data is treated as confidential. As such, all backups and data transfers are encrypted, per policy. Backups and log files are maintained in compliance with the FM Systems Backup Policy for Hosting, which has been provided to OTIM CISO for review.

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	No – one is not required as the information is work related contact information
4.2	Was notice provided to the individual prior to collection of information?	Not applicable since the information collected is work related information.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	They do not as this is not personal or privacy information, but information that is readily available to FHFA staff through one of several sources: existing floor plans with staff names managed by facilities management; names, telephone numbers and division and office information from active directory located on the agency intranet.
4.4	What are the procedures that allow individuals to gain access to their information?	Other than authorized users, no other individuals have access to the system.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Updates and corrections will be made by authorized FHFA personnel.

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 is used within the Deputy Chief Operating Officer's organization by the relocation, OTIM, and facilities staff.

#	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.	No information is shared, unless under lawful court order.
5.3	Is the sharing of PIT 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.	No PII information is being collected nor shared with any other individuals with the deployment of this software. SORNs are for information collected from the public; therefore, a SORN is not required.
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? If so, attach a copy to this PIA.	Client user access is filtered as stated previously in this document User logins are maintained by the FM Interact Administrator(s).
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.	If a server is down. Peak 10 employees may, at the request and direction of FM Systems, enter the FM Systems Rack and do basic diagnostics on the down server. At no time are they given credentials to log into the systems.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	Training for the system is provided by the vendor, ProSource Consulting, LLC as part of their contract with the Agency.
6.4	What technical safeguards are in place to protect the data?	The controls start at the firewall where access to the client's VM is isolated to client specified points of egress. Only required ports are opened to those points. An optional component is a VPN tunnel from each client site. All connections are encrypted via SSL Certificates. Next is that all client data is stored in client specific databases that are secured such that they can only be accessed by the client's logins (FM Support and FM Systems Hosting departments and the FM

#	Question	Response
		Systems Consultant assigned to the project also have access). Per FM Systems Employee Handbook and the Hosting Acceptable Use Policy, all data is treated as confidential. As such, all backups and data transfers are encrypted, per policy.
6.5	What auditing measures are in place to protect the data?	FM Systems Hosting Department audits the permissions on a monthly basis (and after any modifications are made to logins) to ensure that they are in compliance and no access have been granted that should not have been. This is done for both SQL and SSRS. The Audit is reviewed by the hosting department employees and if anything is found to be out of compliance it is corrected immediately as a critical issue. This same audit is also done after every change the effects logins to ensure it not change permissions.
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.	No. However, one is required and in the process of being accomplished by FHFA OTIM IT Security.

Dave Gilson System Owner (Printed Name)	System Owner (Signature)	Nov 9, 2011 Date
N/A COTS System Developer (Printed Name)	System Developer (Signature)	Date
Ralph Mosios Chief Information Security Officer (Printed Name)	Ralph Mosios Chief Information Security Officer (Signature)	Nov 9, 2011 Date
R. Kevin Winkler Chief Information Officer (Printed Name)	Chief Information Officer (Signature)	11/9/11 Date
David A. Lee Chief Privacy Officer (Printed Name)	Chief Privacy Officer (Signature)	11/16/2011 Date

* Note: Questions 2.2 and 6.4. highlight a VPN tunnel/Abut OTIM provided our IP ranges for IP filtering. Therefore, the VPN tunnel option will not be used.