Privacy Impact Assessment Template

FHFA VOICE OVER INTERNET PROTOCOL (VOIP) AND UNIFIED COMMUNICATION (UC)

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
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) 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.

FOR A PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- **Overview**
- **Section 1**
- **Section 2**
- **Section 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 include:
  - 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 Neighborworks).
- 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)(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 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 (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 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 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 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: April 10, 2012

Name of System: FHFA VoIP and UC

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

Name	E-mail	Phone #
Tina Moore	[redacted]@[redacted]	202-[redacted]

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 FHFA Voice over Internet Protocol (VoIP) and Unified Communication (UC) is a set of systems that provides telephone, voice messaging, emergency notifications, and faxing services to FHFA. The VoIP and UC system consist of several servers, software, IP phones, gateways, circuits, and telephone numbers deployed throughout the agency. FHFA Authorized Users, FHFA Offices, IP Phones, and FAX devices are assigned telephone numbers that are configured on the VoIP and UC system and all calls to/from these telephone numbers are transmitted through this system. The VoIP and UC system maintains a listing of telephone numbers and the associated users\offices\devices assigned to the numbers. The system contains voice messaging mailboxes for the delivery and storage of voicemails to users on the VoIP and UC system. There are also telephone numbers associated to the emergency responder system which directs 911 calls from the VoIP and UC system to the internal life safety users and appropriate external public safety answering points.

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?	The system maintains a listing of telephone numbers, phones, gateways, trunks, and end users names. Names of users/offices/devices are assigned to telephone numbers for caller identification purposes. System collects callers telephone number and caller ID information (when available) to be presented to called party. Configuration changes made to the system are also collected.
1.2	What are the sources of the information in the system?	For internal telephone numbers and caller IDs, the source is the Communication Manager. For external telephone numbers and caller IDs (when available), the source is the service provider of the numbers.
1.3	Why is the information being collected, used, disseminated, or maintained?	Telephone numbers and end user IDs are maintained to allow the system to know what user/office/device calls, faxes or where voice messages should be sent. Other telephone numbers, caller IDs, call date\time, and call duration are collected to allow for call history and call detail logging and reporting. Configuration changes such as user logins and logouts, service activations and deactivations, addition\removal of devices, telephone numbers, and end users are collect for audit logging.
1.4	How is the information collected?	The system automatically collects data when calls are placed or received and when configuration changes are made.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Minimal, internal caller ID's and telephone numbers assigned to FHFA are for business purposes. External caller ID's and telephone numbers that are being collected are derived from external telephone service providers and are generally available to the public unless caller has specifically blocked their caller ID 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.	Provides call history on received\missed\placed calls. Provides caller information when calls are placed to 911 to allow for proper call routing. Used in generating call detail reports and audit logs for troubleshooting and auditing purposes.
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.	Accounts with role based reporting and administrative privileges are used to generate call detail reports and access to logs. Individual users can clear their own call history on their phone when necessary.

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?	Call Detail Records are maintained for 30 days. System Audit logs are centrally managed from the real-time monitoring tool. The system maintains a maximum 250 files and when this number is reached the oldest files are purged. The log retention time varies depending on the number of system changes or events but the typical time frame is 6 months.
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.	No.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Call detail records or audit logs could not be easily generated directly from the system if request for data was outside the retentions periods on the system. If records or logs were required outside these periods for investigative purposes retention dates could be changed to retain records and logs for a longer period or logs may be restored from system backups.

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, FHFA-20 – Telecommunications Systems.
4.2	Was notice provided to the individual prior to collection of information?	No.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes, individual callers can specifically block their caller ID information.
4.4	What are the procedures that allow individuals to gain access to their information?	None.
4.5	What are the procedures for correcting inaccurate or erroneous information?	None, data is collected automatically.

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?	OIG or other internal FHFA offices may request call detail records or system audit logs; these reports are gathered for auditing, troubleshooting, or information gathering purposes.
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.	Call detail records or system audit logs will be provided to Federal, state, and local government, and law enforcement agencies for authorized purposes.
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.	Yes. Yes. The sharing is compatible with the routine uses described in the SORN FHFA-20, Telecommunications Systems.

#	Question	Response
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	External data shared with authorized organizations and for legitimate purposes only.

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.	Access to the system is based on role based administration. All users configured in the system can access and make end user changes to their assigned phones and are able to access their voicemail box. Helpdesk staff has been given access to allow for basic administration and OTIM has administrators that have full control of the system. MessageAdmin rights have been granted to Life Safety group to allow them to broadcast public announcement messages through the phones.
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.	Yes contractors within OTIM, Helpdesk and Life Safety group have access to the system via role based administration controls. Procedures are being documented in the Standard Operating Procedures for the system which are under development.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	General end user training was provided when the system was first deployed. Subsequent one-on-one training is provided when requested. Helpdesk staff and Life Safety have been trained on their appropriate administration roles.
6.4	What technical safeguards are in place to protect the data?	Access to the system is via username\password access through secure websites or via secure shell sessions for administration. Access to voicemail from the phones is via a personal pin number. Access to personal address book from the phone is via username\pin.
6.5	What auditing measures are in place to protect the data?	System is part of the General Support System and is scanned accordingly.

#	Question	Response
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.	Security authorization testing and reports completed, authorization official's review and signature expected in April 2012.

Signatures

Tina Moore System Owner (Printed Name)	Tina Moore System Owner (Signature)	4/11/12 Date
N/A System Developer (Printed Name)	System Developer (Signature)	Date
Ralph Mosios Chief Information Security Officer (Printed Name)	Ralph Mosios Chief Information Security Officer (Signature)	4/13/2012 Date
Kevin Winkler Chief Information Officer (Printed Name)	Chief Information Officer (Signature)	4/20/12 Date
David A. Lee Chief Privacy Officer (Printed Name)	Chief Privacy Officer (Signature)	4/23/2012 Date