Privacy Impact Assessment Form

ACCESS CONTROL – EMERGENCY CONTACTS MODULE
(SYSTEM NAME)

This document is only 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 form 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 (PIA)

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is handled. PIAs are to be completed when FHFA: 1) develops or procures IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or 2) initiates a new electronic collection of information in an identifiable form for 10 or more members of the public. System owners and developers are responsible for completing the. The guidance below has been provided to help the system owners and developers complete the PIA.

Overview

- This section should provide a thorough and clear overview of the system and give the reader the appropriate context to understand the system owner's responses in the PIA. 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 will 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, geographic, or financial, with no link to a name or other identifier, such as name, home address, social security number, account number, home telephone and fax numbers, or personal e-mail address.
- Examples of sources of the information include information that comes from individuals applying for loans, mortgages, and forms individuals completed. Where does the data originate? (e.g., the FHA, Office of Personnel Management, and Financial Institutions). 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, an organization).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB's approval to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act of 1980.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports the 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 a limited number of program staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires agencies to address the retention and disposal of information about individuals. (The retention information is published in the Privacy Act system of records notice).
- The retention periods of data/records that the agency manages are contained in either the NARA General Records Schedule or agency Records Schedule. For the data being created/ maintained in the system, the records schedules are the authoritative sources for this information.
- 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 at 5 U.S.C. 552a(e)(1) 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."
- 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 it is a Privacy Act system and may need a system of records notice (SORN published in the Federal Register. The system may already have a Privacy Act SORN that applies to it. If you do not have a published SORN, contact the Privacy Act Officer. The Privacy Act requires that amendments to an existing system must also be addressed in a Federal Register notice. 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.
- 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 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.
- The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

Section 5.0 Sharing and Disclosure

- If it is unknown to you whether or not systems share data, you can either contact the business owner of the data, or you can contact the IT specialist who knows what other interface goes on 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 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 appropriate 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 statutory restrictions on use and disclosure of information that comes from a SORN.

Section 6.0 Technical Access and Security

- For the most part, access to data by a user within FHFA is determined by the "need-to-know" requirements of the Privacy Act (this means to authorized employees within the agency who have a need for the information to perform their duties). Care should be taken to ensure that only those employees who need the information have access to that information. Other considerations are the user's profile based on the user's job requirements and managerial decisions.
- The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?
- 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 may 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.
- The IT Security 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 certain monitoring for authorized reasons by authorized employees. What is in place to ensure that only those authorized can monitor use of the system? For example, business rules, internal instructions, posting Privacy Warning Notices address access controls and violations for unauthorized monitoring and access. It is the responsibility of managers of systems to ensure 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 is explicitly enabled or restricted. It is the responsibility of managers of systems to ensure no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. 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 some sort of control 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 in response to this question.
- Are there privacy and security awareness controls such as training materials for personnel? All employees, including contractors, have requirements for protecting information in Privacy Act systems
- Describe the controls in place to protect the information.

System Name: Access Control – Emergency Contacts Module

System Owner(s):

Name	E-mail	Phone #
Tom Davy	Thomas.davy@fhfa.gov	(202) 408-2897

Overview

The overview section provides an overview of the system and should address the following elements:

- 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;
- A general description of the information in the system.

System Overview
The system is used to maintain emergency contact information for FHFA employees and provides the ability to contact employees in the event of an emergency. The system automates the collection of emergency contact information using the Access Control system. Employees are required to provide a home address and contact information and may provide local and distant emergency contacts. The system is linked to Active Directory and organizes the data according to the organization hierarchy and manager/supervisor assignments. Managers/supervisors, HR, and continuity personnel can view data and run reports.

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, rule, 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?	FHFA employees are required to enter their home address and phone number. They can voluntarily provide an alternate phone number and email address. In addition, they may provide the name, relationship, address, phone number and email address of a local and\or distant emergency contact. Contractors will be asked to provide a business contact phone number and e-mail address.
1.2	What are the sources of the information in the system?	FHFA employees will enter information directly into the web-based application.

#	Question	Response
1.3	Why is the information being collected, used, disseminated, or maintained?	This information will allow FHFA to contact employees' and\or their contacts in the event of an emergency.
1.4	How is the information collected?	This information will be collected via data entry into a web-based application.
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. The information collected will be limited to basic contact information that is already typically available in the public domain.

Section 2.0 Uses of the Information

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

#	Question	Response
2.1	Describe the uses of information.	This information allows FHFA management to contact employees and\or their contacts in the event of an emergency.
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 application is only accessible while connected to the FHFA local area network (i.e., requires a valid FHFA User ID and password to access the system). Employees are the only individuals allowed to enter and maintain their personnel information. Access to employee information is controlled through roles. These roles limit who can see the information entered by a staff member. For example, HR and System administrators can see all staff information, and Managers are allowed to view direct reporting staff information. Ad-hoc access to the data is prohibited unless approved by the system owner.

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?	The emergency contact information will be stored in a distinct set of custom tables within the database. This information may be removed (either hard or soft deletes) as directed in the requirements.
3.2	Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?	Records will be retained in accordance with NARA requirements.
3.3	Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The data retention risk is low. Emergency contact information for staff who have left the agency may remain in the database until their information is removed. This risk is migrated by limiting the data access to staff, their manager and agency continuity of operations personnel. Ad-hoc access to the data is prohibited unless approved by the system owner.

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?	Yes, OPM publishes a government wide SORN OPM GOVT-1 for general personnel records.
4.2	Was notice provided to the individual prior to collection of information?	Yes. A Privacy Act Notice describing FHFAs right to collect this information appears via a pop-up window each time an employee navigates to the data entry form. The user must press the *Close* button before continuing with data entry.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	FHFA employees are required to enter their home address and phone number, but entry of all other information is voluntary.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	The application is only accessible while connected to the FHFA local area network (i.e., requires a valid FHFA User ID and password to access the system). Employees are the only individuals allowed to enter and maintain their personal information.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Employees are the only individuals allowed to enter and correct their personal information. Periodically employees will be asked verify/update their information.

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 entered is available to immediate supervisors, Office of Human Resource Management (OHRM) personnel and agency continuity of operations personnel.
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 from the system will be shared with the agency's alert notification system; however it will be limited to phone numbers and alternate e-mail address.
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, please describe. If not, please describe under what legal authority the program or system is allowed to share the PII outside of the agency.	Yes, OPM GOVT-1 allows sharing of information with agency contractors. Contact information from the system will be used for an automated alert notification system.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Information shared outside the agency will be limited to a contact phone number and alternate e-mail (if provided by the employee). The information will be limited to information required to populate an alert notification system.

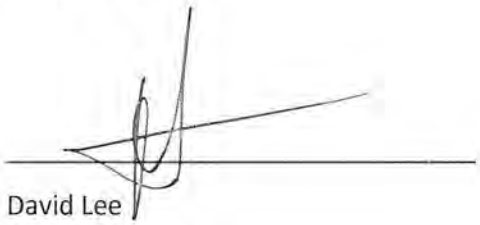
Section 6.0 Technical Access and Security

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 and are these procedures documented?	All employees will have access to the data entry form for data input and maintenance. Members included in the different application roles are documented and maintained through Windows Active Directory.
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?	Yes, contractors will have access to the system for the purpose of entering their business contact phone number and email address (optional). Contractors may gain access to the application while connected to the FHFA local area network (i.e., requires a valid FHFA User ID and password) and entering the URL in their browser. Contractors will not have access to employee information.
6.3	Describe what privacy training is provided to users either generally or specifically relevant to the program or system?	All FHFA employees are required to participate in annual Information System Security Awareness and Privacy Training.
6.4	What technical safeguards are in place to protect the data?	The application data will be stored in an MS SQLServer database located on a secure server. Employees can only access the data through the application as ad-hoc access to the data is prohibited unless approved by the system owner. System and Database administrators will be granted privileges sufficient to successfully complete required tasks.
6.5	What auditing measures are in place to protect the data?	The emergency contact information entered will be stored in a distinct set of custom tables within the database and may be reviewed and audited. The FHFA General Support System (GSS) spans all database and application servers throughout the agency. The GSS is subjected to the Certification and Accreditation process on a yearly basis.
6.6	Has a Certification & Accreditation been completed for the system or systems supporting the program?	Yes. The FHFA General Support System (GSS) spans all database and application servers throughout the agency. The GSS is subjected to the Certification and Accreditation process on a yearly basis.

Access Control – Emergency Contacts Module

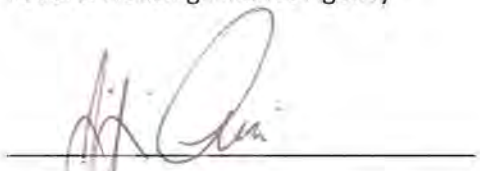
Signature Page



7/23/2010

David Lee
System Owner
Federal Housing Finance Agency

Date



7/1/2010

Jude Corina
System Developer
Federal Housing Finance Agency

Date

8/26/10

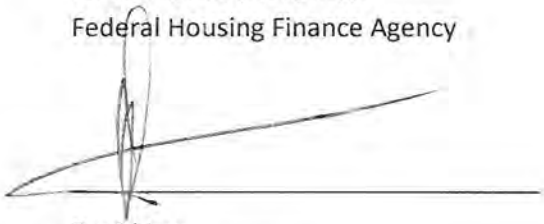
Robert Pirolli
Chief Information Security Officer
Federal Housing Finance Agency

Date

8/26/10

Kevin Winkler
Chief Information Officer
Federal Housing Finance Agency

Date



8/26/2010

David Lee
Chief Privacy Officer
Federal Housing Finance Agency

Date