



Privacy Impact Assessment Template

EMERGENCY NOTIFICATION SYSTEM
(SYSTEM NAME)

JUNE 14, 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 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”; also referred to as 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

- 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: June 14, 2016

System Name: Emergency Communications System			
System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Katrina Jones	Katrina.Jones@fhfa.gov	OFOM	(202) 649-3789
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.			
<p>The Emergency Notification System (ENS) is a critical automated web based notification system used to keep FHFA employees and contractors informed before, during and after an emergency. It allows FHFA to reach multiple individuals at multiple points of contact quickly and efficiently. It also notifies FHFA if, when and how an individual received that message. ENS enhances FHFA’s communications capabilities during an emergency preparedness event and supports FHFA’s ability to determine if an employee or contractor personnel requires help throughout an emergency. The system can be used to push information out to employees and contractor personnel, and supports FHFA in the performance of mission-essential functions before, during and after an emergency preparedness event. FHFA staff in the Office of Facilities Operations Management (OFOM) will have primary responsibility for sending messages and managing the system.</p>			

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?	Names (i.e., individuals). Photographic and/or Biometric Identifiers (i.e., photographs, fingerprints and voiceprints). Personal and Work/Business Telephone Numbers (i.e. telephone, facsimile, and cellular). Addresses (i.e., home, mailing and work/business). Email Addresses (i.e., personal and work/business). Geospatial or Geolocation Data.
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) is taken from Windows Active Directory on FHFA servers. Personal information is voluntarily provided by individuals.
1.3	Why is the information being collected, used, disseminated, or maintained?	The primary purpose is to contact employees and contractors before, during or after an emergency situation in order to deliver a message or to account for FHFA employees and contractors. Additionally, it may be used in non-emergency situations, such as informing FHFA personnel and contractors of office closures due to inclement weather.
1.4	How is the information collected?	FHFA information is taken from the Windows Active Directory on FHFA servers. Personal information is voluntarily provided. ENS allows users to input personal information, such as personal telephone number, personal e-mail, and the names, telephone numbers, and e-mail addresses of emergency contacts.
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, work phone numbers (desk and iPhone/BB) and work e-mail and emergency contact information has the potential of being compromised. Additionally, those who chose to give a

FHFA PIA FOR EMERGENCY NOTIFICATION SYSTEM

#	Question	Response
		"home" phone number and/or personal email address could also have that information compromised. This could result in unwanted contacts.

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.	Information stored in ENS will be used to contact all or a select a group of employees and contractors (personnel) in emergency and non-emergency situations. This might include office closure, natural disaster, or a man-made threat. It will give notice to employees and contractors and will provide senior leadership the ability to account for employees and contractor.
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, Preparedness Program Manager, Chief Operating Officer, Associate Director for Agency Operations, OFOM and authorized OTIM 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. Authorized OTIM IT Security users 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.

FHFA PIA FOR EMERGENCY NOTIFICATION SYSTEM

#	Question	Response
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Once the initial emergency notification database is setup, data updates will be transferred from FHFA directly to the vendor through a point to point method of communications. This will decrease the risk of data loss due to hacking or other nefarious means. The vendor will overwrite the prior data to ensure that departed employee and contractor data is replaced with current and new hire data mitigating the risk of old data being stored. As part of the contract requirement, the vendor will not keep any FHFA data past the end date of the contract. All data will be returned to FHFA at the end of the contract and will be stored within FHFA spaces to meet FHFA OTIM security guidelines and the National Archives records guidelines. The vendor will sanitize applicable storage devices in accordance with NIST 800-88 Revision 1 Guidelines for Media Sanitization. Once the data has been returned to FHFA, the data will be stored and secured by OTIM until the data meets the records retention end date. At this 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.

#	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 -14 – Emergency Notification System published on April 15, 2016. This will need to be updated to reflect new data elements collected, and a new vendor and storage location.
4.2	Was notice provided to the individual prior to collection of information?	Notice is not provided for their work information collected from FHFA systems. Notice is provided before users input their personal information into the system.

FHFA PIA FOR EMERGENCY NOTIFICATION SYSTEM

#	Question	Response
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes. FHFA employees may choose whether to enter their personal information in the program. The removal of FHFA information for a federal employee or contractor is a management call/decision.
4.4	What are the procedures that allow individuals to gain access to their information?	Employees may access their personal information in the system. The System Administrators and the System Owner may also see and update the information. Employees may inform the System Owner that they have recently updated their personal information in the system in order to expedite the delivery of the updated information.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Inaccurate or erroneous information can be corrected by an updated push of information, the administrator, or the user 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 Group since they have responsibility for safeguarding all FHFA information technology, protecting information systems and ensuring confidentiality, integrity, and availability of IT resources. ENS will be available to the System Owner for the purpose of aggregating the data from the Windows Active Directory and sending messages.
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.	The aggregated information from Windows Active Directory will be sent to the vendor responsible for creating, and maintaining the emergency notification system. Also, it will be sent to the vendor so that they can input data into the system. Once they have done this, the vendor will have the ability to send out a message when directed to do so by the System Owner or their designated representative. 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

#	Question	Response
		by Congress; 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 FHFA employee or contractor will have his or her work and (if given), personal telephone numbers and email address 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>	FHFA has developed Access Control and Audit Procedures to govern account management procedures. These procedures are carried out by privileged FHFA users who administer the system and manage all FHFA accounts.

FHFA PIA FOR EMERGENCY NOTIFICATION SYSTEM

#	Question	Response
6.2	<p>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></p>	<p>Yes. Contractors will have access to the system in two ways. First, contractors working within FHFA (i.e., Help Desk Staff) will have access to defined areas within the system. This will allow their personal information to be sent to the vendor in the same way that FHFA employee's personal information is given to the vendor so that they may be contacted in an emergency. FHFA will control their access to the system in the same way that FHFA employee's is controlled, i.e., they may only log on to the system allowing them to manage their personal information. They may only log on to the system while logged on to an FHFA computer, they may not see other employees' personal information, and they may choose to decline to upload any personal information into the system. The second way that contractors have access refers to the contractors at the vendor who provide the service. Their access to the system refers to the information that is provided by FHFA to them. They have the ability to use that information to send out emergency notifications when instructed to do so by an authorized FHFA user. The vendor is contractually obligated not to divulge or misuse the information FHFA provides to them. Other than the contractual relationship between FHFA and the vendor, there is no auditing or enforcement mechanism currently in place to ensure compliance.</p>
6.3	<p>Describe the training that is provided to users either generally or specifically that is relevant to the program or System?</p>	<p>Privileged FHFA users are trained on account management procedures by OTIM Security. The vendor will provide onsite initial system training for FHFA staff. After the initial training, the vendor offers online, over the phone and email help desk support.</p>
6.4	<p>What technical safeguards are in place to protect the data?</p>	<p>Everbridge is currently undergoing the FedRAMP assessment and authorization process. The system is being assessed at the FIPS-199 Moderate Impact Level. FedRAMP requires that all cloud vendors implement a set of controls that exceed the requirements of NIST SP 800-53 Revision 4 to protect agency data in transit and at rest within the Everbridge system. Further, FHFA has developed the Everbridge Access Control and Audit Procedures to define how FHFA privileged users securely manage user accounts and monitor user behavior.</p>

FHFA PIA FOR EMERGENCY NOTIFICATION SYSTEM

#	Question	Response
6.5	What auditing measures are in place to protect the data?	Audit logs are not available to FHFA users within the Everbridge system; however, they can be requested in the case of a suspected security incident.
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.	The Everbridge FedRAMP assessment package has been reviewed by FHFA and FHFA will issue an Agency Authorization to Operate (ATO) in June 2016.

Signatures

Katrina Jones
System Owner (Printed Name)


System Owner (Signature)

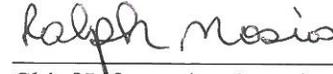
6/15/16
Date

N/A –COTS Product
System Developer (Printed Name)

n/a
System Developer (Signature)

Date

Ralph Mosios
Chief Information Security Officer
(Printed Name)


Chief Information Security Officer
(Signature)

6/20/2016
Date

R. Kevin Winkler
Chief Information Officer
(Printed Name)


Chief Information Officer
(Signature)

6/23/2016
Date

David A. Lee
Chief Privacy Officer
(Printed Name)


Chief Privacy Officer
(Signature)

6/24/2016
Date