Privacy Impact Assessment (PIA) Template

EMERGENCY NOTIFICATION SYSTEM

July 2024

System/Collection Overview
The Emergency Notification System (ENS) is an existing system that is operated by vendor, OnSolve, LLC. 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 requires help throughout an emergency. The system can be used to push information out to employees and contractors 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. Authorized personnel from each program office/division within FHFA will also have the capability to send messages to the employees and contractors in their specific office/division.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	This system collects names, personal contact information, business contact information, division/office assignments, and unique employee identifiers.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The information comes from two sources. Business contact information, division/office assignments, and unique employee identifiers are taken from the FHFA Active Directory, which is in the General Support System (GSS) environment. Personal contact information is voluntarily provided by individuals.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The primary purpose is to contact employees and contractors before, during, or after an agency-wide emergency to deliver a message or to account for FHFA employees and contractors. Additionally, it may be used in agency-wide non-emergency situations, such as informing FHFA employees and contractors of office closures due to inclement weather.

1.4	How is the information provided to or otherwise obtained by the System/Collection?	FHFA/business information is taken from the Active Directory. Personal information is voluntarily provided by individual employees and contractors.
1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	Information stored in ENS will be used to contact all or a select group of employees and contractors in agency-wide emergency and non-emergency situations. This might include an office closure, natural disaster, or man-made threat. It will give notice to employees and contractors and will provide senior leadership the ability to account for employees and contractors.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Only authorized users with a business need-to-know will have access to the information, specifically, the System Owner, Preparedness Program Manager, Chief Operating Officer, Associate Director for Agency Operations, the Deputy Director from each office/division and/or their authorized designee, OFOM, and authorized Office of Technology and Information Management (OTIM) personnel. Authorized administrators will have the ability to run reports, monitor the user and data being requested, and grant and remove user accounts and permissions. Authorized OTIM IT Security users will be able to check/track log files, system penetrations, and misuses of the system.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	Information is destroyed seven (7) years after cutoff. Cutoff occurs when the project/activity/ transaction is completed or superseded.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	Yes. Records are scheduled in FHFA's Comprehensive Records Schedule as Item 5.1 - Administrative Management Records. The NARA Authority for this records schedule is NI-543-11-1.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	Yes. SORN FHFA-14, Emergency Notification System, published on July 31, 2024.
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	SORN FHFA-14 provides notice that the system will collect PII. Additional notice is provided before users input their personal contact information into the system via a Privacy Act notice, which is located on the ENS Home page when accessing the system.
4.3	Is an individual's response to the request for information voluntary or mandatory?	An individual's response to the request for an employee's or contractor's personal contact information is voluntary. However, the collection of an employee's or contractor's business contact information, division/office assignment, and unique employee/contractor identifier is automatically collected from Active Directory without the employee's or contractor's express permission or consent.

4.4	What are the consequences if an individual declines to provide the information?	Employees and contractors who decline to provide their personal contact information may not receive timely notice of an agency-wide emergency or non-emergency event or situation to their personal devices or personal means of contact (e.g., personal email address or phone number).
4.5	What are the procedures that allow individuals to gain access to their information?	Individuals can direct requests for access to the Privacy Office in accordance with FHFA's Privacy Act Regulation, 12 CFR 1204, which is expressly referenced in SORN FHFA-14. The System Administrators and the System Owner may also see and update the employee's or contractor's personal contact information upon request by that employee or contractor.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Individuals can direct requests to correct or amend their contact information to the Privacy Office in accordance with FHFA's Privacy Act Regulation, 12 CFR 1204, which is expressly referenced in SORN FHFA-14. Individuals can contest or appeal an adverse decision for a requested correction or amendment to a record to the Privacy Act Appeals Officer in accordance with FHFA's Privacy Act Regulation, 12 CFR 1204, which is also expressly referenced in SORN FHFA-14. Inaccurate or erroneous information can also be corrected by an updated push of information, or by the administrator or user correcting the information they have inputted.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	The information gathered will be available to OTIM, the System Owner, and other authorized FHFA employees, as described in the response to Question 2.2 above. It will be shared with OTIM, IT Security Group as 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, Preparedness Program Manager, and the Chief Operating Officer for the purpose of aggregating the data from Active Directory and sending necessary messaging. Each FHFA Deputy Director and/or their authorized designee will have access to the contact information in the system in order to send out office/division specific messaging.
5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	The aggregated information from Active Directory will be sent to the vendor responsible for creating and maintaining the ENS 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., Department of Justice (DOJ)/Federal Bureau of Investigation (FBI); Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA); courts; magistrates; members of advisory committees that are created by FHFA or by Congress; members of Congress; other contractor or vendor employees performing or working on a contract; officials of a labor organization; Office of Management and Budget; and the Office of the Inspector General for the FHFA), 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 DHS threat alerts, weather related emergencies, or other critical situations.

5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes. See the routine uses applicable to SORN FHFA-14, Emergency Notification System.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	The employees and/or contractors of the vendor providing services for this information system who have an official need-to-know have access to the information provided to them by FHFA. They are contractually required to use that information to send out emergency notifications when instructed to do so by an authorized FHFA user. The vendor is also contractually prohibited from sharing the information FHFA provides to them with any other person or entity and from using the information for any purpose not expressly authorized by the contract or FHFA. 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.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	No.

6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training for use of FHFA systems at onboarding and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training is required for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII. The vendor will provide virtual initial system training for FHFA staff. After the initial training, the vendor offers online training webinars, telephonic, email help desk support, and quarterly customer connect events.
6.4	Describe the technical/administrative safeguards in place to protect the data.	ENS is authorized under the Federal Risk and Authorization Management Program (FedRAMP). ENS received its initial FedRAMP Authorization on May 12, 2023. It is FedRAMP certified and FHFA reviews the status of ongoing assessments at least annually. FHFA has developed Customer Controls that describe the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating and reviewing audit logs, etc.

Section 7.0 Risk

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

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	In the event of a data loss or mishandled data, the risk to personal privacy of FHFA personnel is that their personal information, specifically their name, work phone numbers (desk and iPhone) and work e-mail and emergency contact information has the potential of being compromised. Additionally, those who chose to give a "home" phone number and/or personal email address could also have that information compromised. The risks of a compromise of the PII collected by ENS include unwanted contacts, harassment, or an attempt(s) at stealing the subject individual's identity. These risks are mitigated by limiting the type of information collected to that which is necessary for the system to properly function in order to accomplish the intended purpose of the system.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The privacy risks associated with the retention of PII is the potential for the individual's data to be lost or compromised. This could result in identity theft, embarrassment, and/or misuse of the individual's personal information. To address these risks, the retention schedule is approved by FHFA's Records Management Office and the National Archives and Records Administration, and access to ENS information is limited to FHFA employees with an official business need-to-know.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	The primary risks associated with the external sharing of the data is that a vendor's employee or contractor will have FHFA employees and/or contractors PII exposed and thus risk identity theft, embarrassment, harassment, or misuse of the person's personal information. Additionally, there could be a potential compromise to the quality or integrity of the PII during the transfer to the external source(s). To mitigate these risks, FHFA OTIM IT Security has established procedures for securely managing access to the application and for reviewing user activity for indications of inappropriate use. They also maintain technical and administrative controls to protect the data during transit.