# Privacy Impact Assessment
for the

# Emergency Notification System (ENS)

## DHS/FEMA/PIA – 036

## April 7, 2014

**Contact Point**

**Melton Roland**
**Office of Response & Recovery (ORR)**
**Response Directorate/Operations Division**
**Federal Emergency Management Agency**
**(540) 665-6152**

**Reviewing Official**

**Karen L. Neuman**
**Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

## Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR), Response Directorate, Operations Division, FEMA Operations Center operates and directs the Emergency Notification System (ENS). This system provides alerts, notifications, warnings, and other similar operations during all hazards, threats, and emergencies to designated FEMA personnel, DHS employees, detailees, contractors, and employees of other participating federal, state, and local agencies and non-governmental organizations (NGO) in the event of a scheduled exercise or an actual emergency. FEMA is conducting this Privacy Impact Assessment (PIA) because ENS collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) in order to provide this service to DHS.

## Overview

FEMA's ORR owns and operates ENS, which has been designated by FEMA Directive 262-3 as the agency solution for all notification and alerts activities. ENS sends notifications and relays messages to DHS employees and contractors, emergency response personnel from other federal agencies, various state and local authorities, and NGOs. These messages are either critical in nature, routine, or for testing purposes with appropriate authorization. In accordance with Executive Order 12656, National Security Presidential Directive (NSPD) - 51[1], Homeland Security Presidential Directive (HSPD) - 20[2], and Federal Continuity Directive (FCD) - 1[3], all DHS organizational components should have a viable Continuity of Operations Planning (COOP) capability and plan in place that ensures the performance of their essential functions during any emergency or situation that could disrupt normal operations. An effective ENS solution is a critical part of this plan.

The National Response Framework (NRF) requires proactive notification and deployment of federal resources in anticipation of or response to all hazards, threats, and emergencies in coordination and collaboration with state, tribal, and local governments, and with private-sector entities when possible. ENS uses communications devices (such as phone, text messages, email messages, and desktop alerts) to share important information in accordance with the NRF and other directives. This information is shared with emergency response personnel from FEMA and other DHS components, federal, state, local, and NGOs in the aftermath of a scheduled exercise or disaster and prompts immediate action to resolve or mitigate the all-hazard situation.

ENS is located at the FEMA Operations Center of the Mount Weather Emergency

[1] http://www.fema.gov/pdf/about/org/ncp/nspd_51.pdf
[2] http://www.fema.gov/pdf/about/org/ncp/nspd_51.pdf
[3] http://www.fema.gov/media-library-data/20130726-1903-25045-0080/fcd_1_october_2012.pdf

Operations Center (MWEOC), which enters into a Memorandum of Understanding (MOU) with each participating DHS component or participating federal, state, and local agency or NGO. The MOU outlines the roles and responsibilities of FEMA and the respective entities. The FEMA Alternate Operations Center East (FAOC-E) in Thomasville, Georgia contains a secondary back-up system, and the FEMA Alternate Operations Center West (FAOC-W) in Denver, Colorado houses a tertiary backup system. FEMA retains the data housed in ENS pursuant to DHS/ALL-014 - Department of Homeland Security Emergency Personnel Location Records System of Records Notice (SORN).[4] National Archives and Records Administration (NARA) General Records Schedule (GRS) - 18, Item 28 and GRS - 20, Items 4 and 5, allow FEMA to delete records when those records are no longer needed for administrative, legal, audit, or other operational purposes.

*Emergency Notification (EN) System Typical Transaction*

DHS employee users input, maintain, and update their own PII in ENS. This data includes name, user ID, login, email addresses, and phone numbers. FEMA designates ENS points of contact (POC) to input necessary information for non-DHS employee users (DHS contractors, representatives of participating federal, state, and local agencies, and NGOs). The POCs are responsible for collecting, importing, maintaining, and updating their respective users' PII in ENS. After a non-DHS employee user's PII is entered into ENS, the user coordinates through his or her POC to maintain and update their information.

The Federal Operations Center provides training for each POC on the verbal privacy notice that POCs are required to give to individuals when providing their PII for ENS. Each POC signs Rules of Behavior that includes guidance about the proper treatment and safeguarding of PII. POCs determine which employees to include in ENS based on their individual emergency response roles and responsibilities. After POCs determine who should be included in ENS, they manually enter the PII into ENS, or individuals submit their information to ENS administrators through an established Microsoft Excel spreadsheet template. Administrators import the PII directly from the spreadsheet into ENS. The Federal Operations Center conducts data imports for larger groups. Each entity (e.g., the POC, DHS component, state and local entity) manages the contacts and data according to its own operational procedures and guidelines. FEMA and Federal Law Enforcement Training Center (FLETC) users have access to ENS and may access and update their information. FEMA provides notice when users provide or update their information through either a verbal Privacy Act Statement from POCs or through a written Privacy Act Statement (on the ENS portal page) prior to collecting the data. All other ENS users continue to coordinate with their respective POC to manage and maintain the accuracy of the PII. POCs delete employees' data from the system when they leave their respective agencies.

[4] DHS/ALL-014 - Department of Homeland Security Emergency Personnel Location Records System of Records, 73 FR 61888 (October 17, 2008).

The Federal Operations Center has a MOU in place with each participating DHS component or participating federal, state, and local agency, or NGO in order to outline the roles and responsibilities of FEMA and the respective entity that maintains a separate ENS database. In the event of an emergency or disaster, FEMA considers the location and circumstances surrounding the incident to determine which FEMA component or office will activate a scenario within the ENS. The activation of a scenario entails sending information, alerts, and instructions intended for a specific audience or group, depending on the situation or emergency. If an emergency affects a particular DHS component, the leadership of that component may choose to activate ENS scenarios according to its COOP or operational plan, as required by the situation. Every FEMA employee is subject to regular and recurring emergency management responsibilities, however not every employee's position requires routine deployment to disaster sites.

ENS sends the users detailed instructions via multiple media (e.g., phone call, text messages, or email) once it has been activated regarding how to respond to notifications (e.g., shelter-in-place, evacuate the area) and tracks whether or not each user has acknowledged receipt of the message. Users respond via key pad on their phones (e.g., pressing "1" for an affirmative response) when instructed to do so, or by replying (e.g., "YES") to the text messages or e-mail message. ENS also uses desktop alerts that are a FEMA-only one-way push and do not allow for responses. FEMA desktop alerts are a supplement to ENS emails, calls, and text messages.

The primary privacy risk associated with ENS is the possibility of erroneous use or disclosure of PII to third parties or external entities. FEMA limits data in ENS to data that is relevant and necessary in order to mitigate the risk of erroneous use of PII. FEMA limits access to PII in the system by using role-based access to ENS. Access to ENS is limited to the approved users, participating organizations POCs, and a few contractor system administrators. These POCs and system administrators are also responsible for removing PII of individuals once they no longer have a role associated with ENS. To mitigate the risk of erroneous disclosure of PII, FEMA only shares the information in ENS outside of DHS pursuant to the routine uses found in DHS/ALL 014 - Emergency Personnel Location Records SORN, through an MOU or Information Sharing Agreement (ISA), or pursuant to a written request submitted to the DHS Headquarters or FEMA Disclosure Office. PII may also be shared with other federal, state, or local government agencies with mission-specific ties to DHS or a component.

## Section 1.0 Authorities and Other Requirements

### 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002,[5] §§ 501-521; the Robert T. Stafford Disaster Relief

[5] P. L. No. 107-296 (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).

and Emergency Assistance Act as amended,[6] §§ 5121–5207; National Security Presidential Directive (NSPD) - 51/Homeland Security Presidential Directive (HSPD) - 20; Federal Continuity Directive (FCD) - 1; and FEMA Directive 262-3.

### 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information collected, stored, and shared by ENS is covered by DHS/ALL - 014 Department of Homeland Security Emergency Personnel Location Records SORN.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Authority to Operate (ATO) for ENS was issued on January 6, 2011, and is currently undergoing recertification.

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS/FEMA retains the information in ENS pursuant to GRS - 18, Item 28 and GRS - 20, Items 4 and 5. Under these schedules, the agency deletes the records when it determines that it no longer needs the records for administrative, legal, audit, or other operational purposes.

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected from federal employees does not require an Office of Management and Budget (OMB) approved collection and number. Any information ENS collects, uses, maintains, retrieves, or disseminates for non-federal employees is covered by OMB through PRA-approved forms. The PRA package for ENS is in the OMB approval process.

## Section 2.0 Characterization of the Information

### 2.1 Identify the information the project collects, uses, disseminates, or maintains.

***Data Elements for Emergency Notification Purposes***

[6] P. L. No. 93-288 (http://www.fema.gov/media-library-data/1383153669955-21f970b19e8eaa67087b7da9f4af706e/stafford_act_booklet_042213_508e.pdf)

ENS uses the following information from DHS employees, detailees, contractors, and employees of other participating federal, state, and local agencies and NGOs:

- User ID;
- Login Name;
- Last Name;
- First Name;
- Middle Initial;
- Agency/Component;
- Company (if applicable);
- Position;
- Email Address(es) (work and personal);
- Email Pager Address(es);
- Work Phone Number(s) (including country code);
- Cell Phone Number(s);
- Comment (text box);
- Fax Number(s) (including country code if applicable);
- Other Number(s) (including country code); and
- Digital Pager Number(s) (including country code).

### 2.2 What are the sources of the information and how is the information collected for the project?

The information is collected directly from DHS employees, detailees, contractors, and employees of other participating federal, state, and local agencies, and NGOs. DHS users initially input information into ENS themselves. Non-DHS users provide their information to designated POCs who manually input or import the information into ENS.

### 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ENS does not use information from commercial sources or publicly available data.

### 2.4 Discuss how accuracy of the data is ensured.

FEMA assumes the initial accuracy of the PII provided by DHS employees, detailees, contractors, and employees of other participating federal, state, and local agencies, NGOs, and their supporting agency or component through input/import. After the initial input/import of PII, individual ENS users are responsible for updating their own PII to ensure its accuracy. POCs are responsible for removing PII of users that leave the organization just as agency or component POCs are responsible for the initial upload of individual users' PII.

### 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a privacy risk that ENS could maintain inaccurate PII on non-federal users because their data is not initially directly collected from them.

**Mitigation:** This privacy risk is mitigated for ENS because POCs get PII directly from individuals and are responsible for the initial upload of non-DHS user's PII, and for removing PII of those users that leave the organization. In addition, when POCs upload the non-users PII, individual users are able to view and update their own PII to ensure accuracy. These POCs coordinate with non-DHS users to correct any inaccurate information.

## Section 3.0 Uses of the Information

### 3.1 Describe how and why the project uses the information.

ENS utilizes user data that is either imported or manually entered into ENS to support deployment operations and to contact federal, state, and local users in the event of an emergency. FEMA or DHS components assess the situation and location of a specific incident to determine which responders to activate in a specific scenario. In a scenario when ENS is activated, users receive the appropriate notifications for the scenario via voice calls to phones, text messages, or as email notifications. Users may respond by acknowledging they have received the message and the explanation of what to do as a result.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

ENS does not and will not use technology to conduct electronic search, queries, or analysis to discover or locate predictive pattern or anomaly.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

Other DHS components have assigned roles and responsibilities within ENS. Each DHS component is required to manage their own personnel data and notifications, and operate the system within their respective areas. For example, Customs and Border Protection (CBP) administrators only have access to CBP information and ability to manage the notifications sent to CBP personnel.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk**: There is a privacy risk that ENS or DHS may keep information for purposes other than the purpose for which it was collected.

**Mitigation**: This risk is mitigated by limiting data in ENS to data that is required to fulfill its response, preparedness, and personnel accountability responsibilities. FEMA uses role-based access that limits access to PII in ENS to individual users, a participating organization's POCs, and a few contractor system administrators to ensure information collection is specific to the identified purpose. POCs and system administrators are also responsible for removing PII of individuals once they are no longer in a role associated with ENS.

## Section 4.0 Notice

### 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

FEMA leverages several types of media to ensure that all individuals receive ample notice that their information will be collected and maintained by ENS. First, the ENS web portal displays a Privacy Act Statement that must be acknowledged before users input data into the system. Furthermore, FEMA forms in the process of being approved by OMB have a Privacy Act Statement (attached at Appendix A). FEMA Directive 262-3, "Emergency Notification System," highlights the purpose, scope, policies and procedures, and information collection by FEMA for ENS purposes. Second, FEMA POCs who enter PII on behalf of responders from non-DHS agencies provide a verbal privacy notice (attached at Appendix B) when they communicate with new users. This communication occurs before these users are added to the system or with current users before updating their PII. Third, FEMA provides training to each new POC includes a section on the Privacy Act Statement. FEMA requires POCs to sign and agree to Rules of Behavior. Finally, this PIA also provides notice of the collection of PII for ENS.

### 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

FEMA employees, detailees, and contractors do not have the opportunity to opt-out of providing PII in ENS due to their specific job duties. Other users (such as participants from other DHS components, federal, state, and local entities, NGOs, non-profit organizations, or other non-employee stakeholders) may omit certain PII fields or may choose to not provide their information to FEMA. Personnel who choose to not provide information will have fewer methods of contact, which will limit their ability to receive notification messages. The respective POCs for each component utilizing the system are responsible for removing PII of any individual who is no longer associated with the sponsoring organization.

### 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk**: There is a privacy risk that the individuals whose PII is included in ENS will not receive notice that their PII is being used for ENS at the time it is collected.

**Mitigation**: This privacy risk is mitigated by providing notice of ENS through: FEMA Directive 262-3; verbal privacy notices to new employees during the on-boarding process; a Privacy Act Statement on the ENS intranet site prior to collection; and by publishing this PIA.

## Section 5.0 Data Retention by the project

### 5.1 Explain how long and for what reason the information is retained.

DHS/FEMA retains information in ENS pursuant to GRS - 18, Item 28; and GRS - 20, Item 4 and 5. Under this rule, records are deleted when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

### 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk**: There is a privacy risk that DHS may keep information in ENS longer than the time period than necessary.

**Mitigation**: DHS mitigates this privacy risk by minimizing the amount of time it keeps the data in line with the mission of its ENS Program. Information is deleted when it is no longer needed. DHS also mitigates this risk by using advanced records management training, additional training offered by DHS and NARA, and advanced technology resources to improve records management practices and functionality.

## Section 6.0 Information Sharing

### 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

DHS does not routinely share ENS information outside of DHS as part of the normal course of operations with the exception of reports that are automatically distributed to authorized ENS users outside of DHS in accordance with mission requirements. DHS may also share information with other federal, state, or local government agencies with mission-specific ties to DHS or DHS components. For example, FEMA may share information with the Urban Search and Rescue teams or state and local officials for situational awareness purposes so that they know which responders are being deployed to the disaster and what time they are expected to arrive. ENS also has the capability to automatically send reports to designated recipients. In order to receive the reports, the recipient must meet several conditions: 1) the recipient must be a contact within the ENS database; 2) the recipient must have the box checked on his/her contact page as being authorized to receive reports; and 3) the recipient must have an e-mail address in ENS.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any sharing of information in ENS is covered by DHS/ALL - 014 Emergency Personnel Location Records SORN. This SORN allows DHS and its components to contact necessary DHS personnel (including federal employees, contractors, and other individuals) to respond to all hazards and emergencies including technical, manmade, or natural disasters, or to participate in exercises. This purpose is consistent with the published routine uses therein, which are compatible with the original purpose of collection.

### 6.3 Does the project place limitations on re-dissemination?

ENS places limitations on re-dissemination. Information is not shared unless covered by a routine use outlined in the DHS/ALL – 014 Emergency Personnel Location Records SORN, or through an approved MOU or ISA.

### 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

ENS maintains a record of report disclosures. Each scenario includes a list of recipients, report types that are sent automatically, and at what interval they were sent out. Requests for ENS records are made to the DHS Headquarters or FEMA Disclosure Office as stated in the DHS/ALL – 014 Emergency Personnel Location Records SORN.

### 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk**: There is a risk that the information in ENS could be erroneously disclosed.

**Mitigation**: DHS mitigates this privacy risk because DHS only shares information in ENS outside of DHS pursuant to the routine uses found in the DHS/ALL - 014 Emergency Personnel Location Records SORN, through an MOU or ISA vetted and approved by the FEMA Privacy Office and Office of Chief Counsel, or pursuant to a written request submitted to the DHS Headquarters or FEMA Disclosure Office. Furthermore, FEMA sends ENS reports to designated recipients who must meet certain conditions prior in order to receive these reports, per section 6.1 above. In addition, FEMA mitigates this risk through training, as all ENS POCs take required system training prior to gaining access to ENS. Lastly, the risk associated with information sharing is mitigated through strict access control measures, as described in section 8.3 below.

## Section 7.0 Redress

### 7.1 What are the procedures that allow individuals to access their information?

PII within ENS is part of the DHS/ALL - 014 Emergency Personnel Location Records SORN. Individuals seeking access to their records may access their information via a Privacy Act or Freedom of Information Act (FOIA) request to the FEMA Disclosure Office. Designated POCs, administrators, creators, and users that have rights to the system can view or update their own and other users' information. All users may view and update their own information because they have their own login IDs and passwords.

### 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

ENS users may correct inaccurate data via the processes noted in Section 7.1 of this PIA. Designated POCs, administrators, creators, and users who have rights to the system can view or update their own PII as well as PII of other users under their authority. Users with their own login ID and password are also able to view and update their own information.

### 7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA along with the SORN provides notice regarding information correction procedures for ENS. FEMA provides a Privacy Act statement in user manuals and to users prior to entering or updating their PII in ENS.

### 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk**: There is a risk that ENS users will be unaware of the redress process available to them.

**Mitigation**: DHS mitigates this privacy risk by providing mechanisms for redress in user manuals and as part of the training for new POCs. This PIA and the DHS/ALL - 014 Emergency Personnel Location Records SORN also offer notice of redress to individuals.

## Section 8.0 Auditing and Accountability

### 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

DHS ensures that the practices stated in this PIA are followed by leveraging standard operating procedures (SOP), training, policies, rules of behavior, and auditing and accountability. FEMA updates ENS documentation annually. FEMA also hosts an annual training conference for ENS POCs.

### 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS/FEMA ENS users are required to successfully meet annual privacy awareness and information security training requirements according the DHS/FEMA training guidelines, as well as program-specific ENS training. Each ENS POC completes a system-oriented training that includes privacy.

### 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ENS uses a role-based access control mechanism for data and functionality. Permissions for the data and functions used to manipulate the data have been pre-defined for each type of user based on the principles of separation of duties and “need to know”. DHS employees, FEMA employees, and authorized non-DHS users authorized Information Technology (IT) contractors will have restricted, role-based, access to ENS only to the extent necessary to perform official duties. IT contractors handling operations and maintenance of the system will also have limited access to ENS to support the troubleshooting of technical system issues encountered on a day-to-day basis. All internal end-users are required to read and sign a Rules of Behavior agreement. There are SOPs for reference and an information system security officer (ISSO) who provides security guidance over the project.

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ENS leverages MOUs and ISAs to facilitate the information exchange necessary to accomplish its mission. All MOUs and ISAs between FEMA and its partners are reviewed by responsible program managers, senior-level stakeholders, DHS and component privacy officers, IT Security staff, the Federal Operations Center Director, and appropriate legal counsel. Finally, DHS formally reviews and approves MOUs and ISAs.

## Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

## Approval Signature

Original signed and on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

## APPENDIX A: PRIVACY NOTICE

**Authority:** The Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 501-521; the Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended, 42 U.S.C. §§ 5121–5207; National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20; Federal Continuity Directive (FCD)-1; and FEMA Directive 262-3 authorize the collection of this information.

**Purpose:** FEMA is collecting this information to ensure that the Emergency Notification System (ENS) has the most current personal contact information for emergency responders in the event of a man-made disaster, a natural disaster, or planned exercise.

**Routine Uses:** FEMA will use this information to send notifications, alerts, and/or activations and to relay critical updates and guidance to DHS personnel, other federal departments, and other agencies or non-governmental organizations in response to an emergency scenario or exercise.

**Disclosure:** Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from receiving notifications in the event of an emergency.

## APPENDIX B: VERBAL PRIVACY NOTICE

“We are required by law to provide the following Privacy Notice to you. The information that you give the Department of Homeland Security, Federal Emergency Management Agency, is collected under the Homeland Security Act of 2002, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, and other authorities. It will be used to send notifications, alerts, and/or activations and to relay critical updates and guidance to DHS personnel, other federal departments, and other agencies or non-governmental organizations in response to an emergency scenario or exercise. DHS/FEMA may share this information outside the agency upon written request, by agreement, or as required by law. Furnishing the requested information is voluntary, however, failure to provide accurate information may delay or prevent the individual from receiving notifications in the event of an emergency.”