Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Emergency Notification System (ENS) (1660-NW49)**		
Component:	Federal Emergency Management Agency (FEMA)	**Office or Program:**	Office of Response & Recovery (ORR)/Response Directorate/Mount Weather Emergency Operations Center (MWEOC)/FEMA Operations Center (FOC)
Xacta FISMA Name (if applicable):	**Emergency Notification System (ENS)**	**Xacta FISMA Number (if applicable):**	FEM-00164-MAJ-00164
Type of Project or Program:	**IT System**	**Project or program status:**	**Existing**
Date first developed:	**August 1, 2000**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**July 31, 2012**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	**January 31, 2013**

PROJECT OR PROGRAM MANAGER

Name:	**Melton Roland**		
Office:	**FEMA Operations Center (FOC)**	**Title:**	ENS Program Manager
Phone:	**540-665-6152**	**Email:**	melton.roland@fema.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**John Shaffer**		
Phone:	**540-665-6293**	**Email:**	john.shaffer@fema.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

The FEMA Office of Response and Recovery (ORR)/Response Directorate owns and operates the Emergency Notification System (ENS), which has been designated by FEMA Directive 262-3 as the agency solution for all notification and alerts activities. Based on operational requirements and in the event of a scheduled exercise or actual disaster, ENS sends alerts, notifications, and relays messages to DHS employees and contractors as well as emergency response personnel in other federal, state, local, and tribal agencies, non-governmental organizations and the private sector. ENS utilizes communications devices such as personal digital assistants (PDAs), alpha pagers, numeric pagers, cell phones (voice and text messages), home phones, work phones, and Blackberries.

In accordance with Exec. Order No. 12656, National Security Presidential Directive (NSPD)-51, Homeland Security Presidential Directive (HSPD)-20 and Federal Continuity Directive (FCD)-1, all DHS organizational components must utilize a Continuity of Operations Planning (COOP) capability and plan to ensure the performance of their essential functions during any emergency or situation that could disrupt normal operations. In addition, the National Response Framework (NRF) requires proactive notification and deployment of federal resources in anticipation of or in response to all hazards, threats, and emergencies in coordination and collaboration with state, tribal, and local governments, and private-sector entities when possible.

The primary ENS system (ENS1) operates within the FEMA Operation Center (FOC) at the Mount Weather Emergency Operations Center (MWEOC), which enters into Memoranda of Understanding (MOUs) with each participating DHS component in order to define respective roles and responsibilities. A secondary, back-up system (ENS2) is located in the FEMA Alternate Operations Center East (FAOC-E) in Thomasville, Georgia, and a tertiary back-up system (ENS3) is located in the Denver MERS Operations Center (FAOC-W). ENS1 replicates data every four hours to both ENS2 and ENS3, which maintain a replica of all personnel contact information, scenarios, groups, etc. These scenarios, known as notification activations, can be initiated on any of the systems. In the event of a disruption to ENS1, then ENS2 or ENS3 would be utilized in a seamless manner. Thus ENS maintains a constant state of readiness.

FEMA retains the data housed in ENS pursuant to DHS/ALL-014 - Department of Homeland Security Emergency Personnel Location System of Records, 73 Fed. Reg. 61,888 (Oct. 17, 2008). Additionally, General Records Schedule (GRS)-18, Item 28 and GRS-20, Items 4 and 5 allow FEMA to delete records when FEMA determines that those records are no longer needed for administrative, legal, audit, or other operational purposes.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☒ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?

DHS employees, contractors, and members of the public all provide the same data elements to be included in ENS. The list below includes the required data elements:

- First Name
- Last Name
- Work E-mail Address
- Personal E-mail Address
- Work Phone
- Home Phone
- Work Cell Phone
- Personal Cell Phone Personal Pager Number
- Personal Pager PIN
- SMS/Text number
- Work Physical Address (optional)
- Home Physical Address (optional)

4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use	☒ No.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

Social Security Numbers (SSN)?	☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: When ENS users are assigned a new role, the ENS Team provides role-based training to explain the role (i.e., Administrators, Creators, and Users). In addition, refresher training is provided to users upon request.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system	☐ No. What steps will be taken to develop and maintain

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.
[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	the accounting: ☒ Yes. In what format is the accounting maintained: All records and requests are maintained by the FEMA Records Management Division/Disclosure Branch.
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**John K. Cook**
Date submitted to Component Privacy Office:	March 4, 2014
Date submitted to DHS Privacy Office:	April 30, 2014
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
PIA: DHS/FEMA/PIA-Emergency Notification System (in process) SORN: DHS/ALL – 014 Emergency Personnel Location Records System of Records	

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Jameson Morgan**
PCTS Workflow Number:	**1018043**
Date approved by DHS Privacy Office:	May 12, 2014
PTA Expiration Date	May 12, 2017

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.

Determination:

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☐ Privacy Act Statement required.

☒ Privacy Impact Assessment (PIA) required.

☒ System of Records Notice (SORN) required.

☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

☐ A Records Schedule may be required. Contact your component Records Officer.

PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/FEMA/PIA – 035 Emergency Notification System
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ALL-014 - Department of Homeland Security Emergency Personnel Location Records System of Records

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

The DHS Privacy Office agrees with the FEMA Privacy Office's recommendation that ENS is a privacy sensitive system with coverage required under the DHS/FEMA/PIA – 035 ENS PIA and the DHS/ALL – 014 Emergency Personnel Location Records System SORN.

This PTA was submitted because ENS was updated and now collects PII from members of the public in addition to employees and contractors. Furthermore, the DHS/FEMA/PIA – 035 ENS PIA was published and provides coverage to this system. The DHS/FEMA/PIA – 035 PIA allows FEMA to provide 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. The DHS/ALL – 014 SORN allows FEMA to contact necessary DHS personnel, including Federal employees and contractors, and other individuals to respond to all hazards emergencies including technical, manmade or natural disasters, or to participate in exercises. The SORN also allows FEMA to facilitate the contact of DHS personnel's families or other in the event of a personal emergency such as an injury concerning the workplace.