

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Emergency Alert Notification System (ENS)

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

11/28/17

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
- From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Department of Defense Office of Inspector General (DoD OIG), Mission Support Team (MST), Logistics Management Office (LMO), operates and directs the agencies Emergency Notification System (ENS). This system provides alerts, notifications, warnings, and other similar operations during all hazards, threats, and emergencies to designated DoD OIG employees in the event of a scheduled exercise or an actual emergency.

MST LMO collects basic contact information to perform this function, including employee's name, component/assigned office, personal cell number, home address, home telephone number, and personal email address.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

The PII selected is collected because it is necessary to ensure mass warning and personnel accountability during emergency situations. Multiple contact points are collected from individuals to maximize the probability of timely notification and accountability.

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

During initial entry into the agency, employees are requested to input their contact information in the Emergency Alert Notification Program, including, personal cell phone number, home telephone number, and personal email address. However, employees can, and have, opted out of the notification program without consequence; in these cases it is up to them to work out an alternative means of notification and accountability with their supervisor.

f. Do individuals have the opportunity to consent to the specific uses of their PII? Yes No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PII is only used to notify employees and establish accountability. Employees can opt out of the the program and request removal of their PII at any time.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- Privacy Act Statement Privacy Advisory Not Applicable

Upon collection, employees are informed that their PII is being collected solely for emergency notification and accountability and will not be used for any other purpose.

Additionally, the website that houses the information has several privacy statements, including below:

"When we retain and process personally identifiable information, we will make certain information available to those individuals on a reasonable and timely basis. This information will include what personal information is being collected, who is collecting it, how and for what purposes it is being collected, how it is being used and to whom it will be disclosed. Any time we request personal information from you, SEND WORD NOW will include a link to this Privacy Policy. When you use our service, communicate with our support team or e-mail us, we may need to get contact information, such as your e-mail address, home and mobile phone numbers. When you submit a question on line, or report a problem with our products or services, we may ask for your name, mailing address, telephone number, or e-mail address, in order to facilitate a speedy response."

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- | | | |
|---|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | Chief of Staff, Security, and potentially other leadership in the case of an actual emergency |
| <input type="checkbox"/> Other DoD Components | Specify. | |
| <input type="checkbox"/> Other Federal Agencies | Specify. | |
| <input type="checkbox"/> State and Local Agencies | Specify. | |
| <input checked="" type="checkbox"/> Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) | Specify. | Send Word Now (SWN) Communications Inc. Privacy Statement states they will not use PII except for the function of fulfilling agencies notification and accountability purpose. |
| <input type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | |

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- | | |
|--|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input checked="" type="checkbox"/> Other (If Other, enter the information in the box below) | |

The system program manager (PM) manually inputs the employees name, component/assigned office, and work location.

Employees are sent a link to input their own PII. They are provided the opportunity to input personal cell number, home address, and home telephone number. They also provide their mailing address via e-mail or phone to the system PM to be inputted into their profile.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

- Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

i. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).
 - (a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.
 - (c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

Presidential Policy Directive 40 - National Continuity Policy, dated July 15, 2016;

Department of Defense Instruction (DoDI) 6055.17, DoD Emergency Management (EM) Program, dated February 13, 2017;

DoDI 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters, dated May 3, 2017;

Inspector General Instruction 3001.02, Personnel Accountability Program, dated August 5, 2016.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB control number not required, system does not collect records from 10 or more members of the public in a 12-month period.