



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Emergency Alert Notification System (EANS)
--

Headquarters, Department of the Army (HQDA) Directorate of Mission Assurance, OAA

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

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

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

10 U.S.C. 3013, Secretary of the Army; E.O. 12656, Assignment of Emergency Preparedness Responsibilities; DoD Directive 3020.26, Continuity of Operations Policy and Planning; and Army Regulation 500-3, Army Continuity of Operations.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

This web-based information system is used to initiate and transmit emergency alerts and notifications in support of the HQDA COOP and EM programs. Alerts are transmitted via phone, e-mail, text message, and blackberry pin-to-pin. Using the HQDA EANS, user organizations can simultaneously contact thousands of personnel on up to 10 devices each (5 voice and 5 text). In addition to sending the alert messages, user organizations can view reports providing real-time individualized confirmation that alerts were received, along with updated personal status for each message recipient.
The personal information collected consists of personal and work-related information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The primary risk to privacy is the unauthorized release of an individual's name, phone number(s) or e-mail address (es).
Contact data is protected throughout every step in the data collection, storage and operation use process. At no point is the data accessible in unencrypted form, nor is it transmitted across non-secure internet channels. The data is accessed only through the EANS, and is used only for the purpose of generating voice-based alert messages (to landline or mobile phones) or text-based alert messages (to e-mail systems, pagers, SMS text devices, Personal Data Assistant (PDA), Blackberry's, etc.). Both the voice and text messages are generated behind the firewall at the vendor facility using Internet Protocol (IP) based technologies, and once placed on the public telephone or internet network, they are encrypted. Each subscriber organization has control over the contact data within their account.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Contact data may be shared internally with authorized personnel who need to contact individuals for EANS purposes.

Other DoD Components.

Specify.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Criminal Investigative Service, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

Other Federal Agencies.

Specify.

In accordance with DoD blanket routine uses, other federal agencies that would obtain access to PII in this system, on request in support of an authorized investigation, audit or other official function, may include appropriate law enforcement agencies, congressional offices, the Office of Management and Budget (OMB), the Office of Personnel Management

(OPM), the Department of Justice (DOJ), the General Services Administration (GSA), and the National Archives and Records Administration.

State and Local Agencies.

Specify.

In accordance with DoD blanket routine uses, state and local agencies that would obtain access to PII in this system, on request in support of an authorized investigation, audit or other official functions, may include appropriate law enforcement agencies and authorized taxing authorities.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Contractors would obtain access to PII in this system in support of performing official duties. This may include approved HQDA contract vendors and SWN Communications, Inc. (SWN). Support contracts include PII protection requirements that are equivalent to those established for DoD personnel, including training, and technical and administrative controls.

Other (e.g., commercial providers, colleges).

Specify.

In accordance with DoD blanket routine uses, other entities that would obtain access to PII in this system, on request in support of an authorized investigation, audit or other official functions, may include law enforcement, security, investigatory, or administrative authorities, and appropriate agencies, entities, and persons in response to suspected or confirmed compromise of information security or confidentiality.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes **No**

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

The individual is furnished a Privacy Act statement and elects to enter data. The language contained in the e-mail message that provides the URL link contains standard language that explains individual privacy rights, including the right not to provide additional personal contact information.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Individuals enter their personal contact information by completing a web-based "Self-Update" process. The Self-Update page includes a Terms and Conditions statement, and individuals are required to check the box acknowledging that they have read, understand, and agree to the terms before they can complete the process. The Terms and Conditions contain standard PIA language covering Authority, Principal Purpose, Routine Use, and Disclosure, as well as the following statement: "By completing the Self-Update process, and clicking on either "No Changes" or "Update," you are granting consent to the use of your personal contact information for the purpose described above.

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

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Notice

When HQDA, Directorate of Mission Assurance, OAA retain and process personally identifiable information 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, SWN 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 online, 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.