



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Emergency Evacuation Tracking and Repatriation

Defense Manpower Data Center

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.

E.O. 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988; DoD Directive 3025.14, Protection and Evacuation of U.S. Citizens and Designated Aliens in Danger Areas Abroad; and E.O. 9397 (SSN).

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.

The records for the Non-combatant Tracking System (NTS) and the Emergency Tracking and Accountability System (ETAS) are maintained for the purposes of tracking and accounting for individuals evacuated from emergency situations overseas and in the United States, securing relocation and assistance services, and accessing and recovering relocation costs. The types of personal information being collected on individuals include: Name, Date of Birth, Social Security Number, Passport Number, Country of Citizenship and gender as well as those listed in Section 3 of this PIA.

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

The privacy risks associated with the PII collected are low based on the physical, administrative and technical safeguards in place as noted in section 3(d) of this PIA.

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.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

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

Specify.

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.

Providing PII is voluntary, but failure to do so may result in delay of evacuation. If objecting at a later date the process described in the SORN is as follows: The OSD (Office of the Secretary of Defense) rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the Privacy Act Officer, Office of Freedom of Information, Washington Headquarters Services, 1155 Defense Pentagon, Washington, D.C. 20301-1155.

(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.

A Privacy Act Statement is posted at evacuation sites. Providing PII is voluntary, but failure to do so may result in delay of evacuation.

(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.

- Privacy Act Statement Privacy Advisory
 Other None

Describe each applicable format.

Authority: E.O. 12656, Assignment of Emergency Preparedness Responsibilities, 18 Nov 1988; DoD Directive 3025.14, Protection and Evacuation of U.S. Citizens and Designated Aliens in Danger Areas Abroad; E.O. 9397 (SSN).

Purpose: The records are maintained for the purposes of tracking and accounting for individuals evacuated from emergency situations in foreign countries, securing relocation and assistance services and assessing and recovering relocation costs.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To individuals who have been evacuated but who have been separated from their family and/or spouse. Information will be released to the individual indicating where the family member was evacuated from and final destination.

To Department of State to plan and monitor evacuation effectiveness and need for services and to verify the number of people by category who have been evacuated.

To the American Red Cross so that upon receipt of information from a repatriation center that a DoD family has arrived safely in the U.S., the Red Cross may notify the service member (sponsor) still in the foreign country that his/her family has safely arrived in the United States.

To the Department of Homeland Security – U.S. Citizenship and Immigration Services to track and make contact with all foreign nationals who have been evacuated to the U.S.

To the Department of Health and Human Services for purposes of giving financial assistance and recoupment of same. To identify individuals who might arrive with an illness which would require quarantine.

Disclosure: Voluntary; however, failure to provide information may result in delays.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.