



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

0704-0334

Enter Expiration Date

07/31/2014

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, 1988as amended; DoD Directive 3025.14, Evacuation of U.S. Citizens and Designated Aliens in Danger from Threatened Areas Abroad; and E.O. 9397 (SSN), as amended

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.

Repatriation centers will use this information to track and account for individuals evacuated from emergency situations and assist in securing requested relocation and assistance services, and recording and recovering relocation costs.

Types of personal information includes: Name, Social Security Number (SSN), date of birth, place of birth, gender, country of citizenship, marital status, sponsor data, passport number and country of issue, alien number and country of issue, country evacuated from, (same information is reported for each family member). Also collected are type of evacuee and an agency code identifying DoD or other U.S. Federal Agency sponsorship, final destination and point of contact name and contact information, emergency contact name and contact information, and identification of any services requested.

(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. Computerized records are maintained in a controlled area accessible only to authorized personnel. At Defense Manpower Data Center (DMDC), entry to these areas is restricted by the use of locks, guards, and administrative procedures. Access to personal information is limited to those who require the records in the performance of their official duties. Access to personal information is further restricted by the use of passwords which are changed periodically.

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.

Department of State, Department of Health and Human Services, Internal Revenue Service, US Citizenship and Immigration Service (USCIS)

State and Local Agencies.

Specify.

State and Local health departments

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

Specify.

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

Specify.

American Red Cross, Family members who have become separated due to emergency evacuation

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, however, failure to furnish the information may limit receipt of services and impede passage of information about individual's current whereabouts to family members.

(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 provided to the individual upon request of their PII. however, failure to furnish the information may limit receipt of services and impede passage of information about individual's current whereabouts to family members.

(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.

AUTHORITY: E.O. 12656; DoD Directive 3025.14, Evacuation of U.S. Citizens and Designated Aliens from Threatened Areas Abroad; and E.O. 9397.

PRINCIPAL PURPOSE(S): To document the movement of an evacuee from a foreign country to an announced safe haven. Information will be used, as needed, to assist the evacuee in the process of repatriation. This information is covered under DMDC 04, Evacuation and Repatriation (<http://dpclod.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/6695/dmdc-04.aspx>).

ROUTINE USE(S): To family members of individuals who have been evacuated and about whom information is requested by a family member and/or spouse, location and final destination will be released; to the Department of State for evacuation management and planning purposes; to the American Red Cross for communication of evacuation information about spouse/family member(s) to service member still in foreign country; to the U.S. Citizenship and Immigration Services (USCIS) for tracking and contacting foreign nationals evacuated to the U.S.; to the Department of Health and Human Services to facilitate delivery of personal and financial services and to recoup costs of financial services and to identify individuals who might arrive with an illness requiring quarantine; to state and local health departments, to further implement the quarantine of an ill individual. The DoD "Blanket Routine Uses" found at <http://dpclod.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> also apply to this system.

DISCLOSURE: Voluntary; however, failure to furnish the information may limit your receipt of services and impede passage of information about your current whereabouts to family members. Social Security Number (SSN) is used in the documentation of payments and loans provided in the process of evacuation and may be provided to the IRS if payment is not received. The Social Security Number (SSN) may also be used in the process of verifying an individual's identity and citizenship.

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.