



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Data Environment/Global Transportation Network Convergence (IGC)

USTRANSCOM

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

FR Doc. E8-13227

Enter Expiration Date

N/A

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. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; DoD Regulation 4500.9E, Transportation and Traffic Management; 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.

To track DOD cargo and personnel moving within the Defense Transportation System (DTS) both in time of peace and war. DTS is DOD transportation infrastructure which supports Department of Defense common user transportation needs across the range of military operations.

Routine Uses of records maintained in the system, including categories of users and the purposes of such uses: The Department of Defense `Blanket Routine Uses' published at the beginning of the Air Force's compilation of systems of records notices apply to this system.

The types of PII used are: Name, Social Security Number, Home Address, Medical Information, Spouse Information, Children Information, Employment information, Gender, Blood type

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

There are no additional privacy risks associated within IGC: The system does not directly collect PIIs from the individuals; receives PII via system interfaces. Design considerations took into account protection of PIIs as did the choice of locations for data storage. Records will be maintained in a DISA secure data facility and is accessible only to authorized personnel. All data is encrypted during transmission. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by enabling Public Key.

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.

IGC receives PII via system interfaces, therefore, IGC has no contact (direct or indirect) with the individuals concerned. However, the originating systems provide the individual the opportunity to object to collection of the PII.

(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.

IGC receives PII via system interfaces, therefore, IGC has no contact (direct or indirect) with the individuals concerned. However, the originating systems provide banners to inform the authority for and to individuals to consent to PII collection. Also, the banners provide the principle purpose for which the PII is intended to be used, the routine uses which may be made of the PII, and the effects on the individual, if any, of not providing all or any part of the requested PII IAW the Privacy Act of 1974.

(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.

IGC receives PII via system interfaces, therefore, IGC has no contact with the individuals concerned. However, the originating systems provides the following three Privacy Act Statements.

PRIVACY ACT STATEMENT I:

AUTHORITY: 10 U.S.C. 8013; EO 9397, 23 November 1943.

PRINCIPAL PURPOSE: To apply for air travel. SSN is needed for positive ID.

ROUTINE USE(S): Records from this system of records may be disclosed for any of the blanket routine uses published by the Air Force.

DISCLOSURE IS VOLUNTARY: Failure to provide the information may result in member not being accepted for travel on military aircraft. Disclosure of SSN is voluntary.

PRIVACY ACT STATEMENT II:

AUTHORITY: 10 U.S.C. Section 113 & Section 5041; EO 9397 (SSN)

PRINCIPAL PURPOSE: This information will be used to verify the identify of eligible users of the MarineNet MDSS II and to set user privileges. SSN is needed to compared the user information in Defense Manpower Data Center and the Marine Corps Total force Structure Systems.

ROUTINE USE(S): None. The "Blanket Routine Uses" set forth by the Department of Defense.

DISCLOSURE: Voluntary. However, failure to provide the requested information will results in denial of access to the system.

PRIVACY ACT STATEMENT III:

AUTHORITY: 10 U.S.C. Section 3013 and E.O. 9397.

PRINCIPAL PURPOSE(s): To provide support to rapid military force deployment planning and execution at the tactical and operational level.

ROUTINE USE(S): None. The "Blanket Routine Uses" set forth at the beginning of the Army's Compilation of Systems of Record Notices also applies to this system.

DISCLOSURE: Voluntary. However, failure to provide all the requested information could provide inadequate data to the Marine Air Ground Task Force Commanders.

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.