



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Transportation Information System (TIS) Enterprise

Department of the Army/ Program Executive Office (PEO) Enterprise Information Systems
(EIS) Product Director Transportation Information System (PD TIS)

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

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 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.

TIS Enterprise is an automated information system that imports personally identifiable information (PII) from Electronic Military Personnel Office (E-MILPO). It provides the Army the capability of transporting materials and personnel. The mission of the Enterprise is to provide an information system that supports the movement of personnel, equipment and sustainment cargo from home to destination and back while maintaining visibility of the movement of tactical, operational and strategic levels. The Enterprise is composed of an Enterprise Management System (EMS), Demilitarized Zones (DMZs), distributed Regional Access Nodes (RANs), a Government Test environment and an Engineering Environment. The operational environment (EMS, DMZ, RANs) is a collection of networked application and data servers which include Transportation Coordinators' Automated Information for Movements System II (TC-AIMS II), Automated Air Load Planning System (AALPS), Transportation Information Systems - Theater Operations (TIS-TO), and Transportation Coordinator's Automated Command & Control Information System (TC ACCIS) and which securely deliver information to the user's web browser. TC-AIMS II and AALPS also have a Breakaway instantiation that supports users without access to the Enterprise.

The EMS manages all the components of the TIS Enterprise and has management subcomponents collated with each RAN. Each of the RANs (e.g., RAN1 and RAN2) is supported by a DMZ (e.g., DMZ1 and DMZ2) which provides the web server interface for Enterprise users as well as a proxy server for brokering data exchange with external systems. The EMS, DMZs and RANs are commonly referred to as the Operational environment. The Government Test environment supports Government verification and validation testing, developmental testing and operational testing of products as required. All delivered products and prototyping of selected products are tested thoroughly in the Government Test environment prior to fielding and implementation. The Engineering environment is employed by the development contractors to perform final integration and testing of hardware and software system components within the Enterprise configuration. The Engineering environment is also where final Test and Integration testing occurs prior to delivery to the Government.

PII information stored can include personal, medical, employment, educational, and military information.

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

The TIS Enterprise installation consists of Citrix Secure Gateway, web servers, database servers and application servers. All servers are configured with Microsoft Windows Server 2003 R2 and hardened with the latest Army Gold Master (AGM) and the appropriate DISA Security Technical Implementation Guides (STIGS). The external users access the enterprise via the web using Hypertext Protocol with Secure Sockets Layer (HTTPS). Information exchange between applications and database is performed by many Virtual Local Area Networks (VLAN). PD TIS implements a Defense in Depth strategy and a restrictive network architecture that only allows authorized traffic. TIS Enterprise is located in a secure facility which has 24/7 monitoring and access controlled server room, and cameras throughout the facility.

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.

Department of the Army, Human Resources Command, Army National Guard; Army Staff Principals in the chain of command, and Supervisors. Army Reserve, and any User Account Manager (UAM), Transportation Officer, or other designated individual involved with supporting unit moves to/from:

Fort Lewis, Fort Irwin, Camp Roberts, Fort Huachuca, Fort Carson, Fort Bliss, Fort Hood, Fort Sill, Fort Riley, Fort McCoy, Fort Leonard Wood, Fort Polk, Fort Campbell, Fort Knox, Fort Rucker, Fort Benning, Fort Stewart, Fort Bragg, Fort Lee, Fort Eustis, Aberdeen Proving Ground, Fort Dix, Fort Drum, Fort Wainwright, Fort Richardson, Fort Buchanan, Iraq, Kuwait, Afghanistan.

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.

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

Since data are not collected directly from individual they are not provided either a Privacy Act Statement or a Privacy Advisory. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

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.

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

Individuals provide the information at the request of their commanders to perform specific duties assigned by in their organizations. The opportunity to object or consent to the collection of the data would have to be provided at the time of duty appointment or enlistment to the Armed Forces.

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

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

Describe each applicable format.