



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Transportation Information System (TIS) Breakaway

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 Breakaway 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 Breakaway 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. TIS Breakaway systems are portable.

The TIS Breakaway installation consists of a standalone laptop configured with Microsoft XP operating system, Sybase database and both TC-AIMS II and AALPS applications. The applications provide a graphical user interface in which mandatory fields are populated from the reference database.

PII is referenced by Unit Identification Code (UIC). 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.

Only users with appropriate roles and permissions are allowed access to the system admin database where PII data is stored. All standalone systems have full disk encryption to protect PII data in transit. The standalone laptop can be connected to the network in client server mode at the local Directorate of Installation Management (DOIM). PD TIS provides the Common Access Card (CAC) authentication software but it is the local DOIM's responsibility to CAC enforce the breakaway system.

The TIS Garrison client/server deployment mode allows the unit to retain and manage data at the local installation level. Garrison servers are configured with Windows 2003 R2 and hardened with Army Gold Master and DISA STIGS. Post-fielding system maintenance and user account access to the software is managed by a PD TIS trained local System Administrator/Database Administrator (SA/DBA). IAVAs are tested by the PMO for applicability to TIS Systems and posted for the SA/DBA to apply to the unit's local server. All the data resides at the server level unless the client system is converted to breakaway mode via data export. Client systems are encrypted with the Mobile Armor DAR solution.

**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.

Army National Guard, 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.

N/A

**Other Federal Agencies.**

Specify.

N/A

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

Describe each applicable format.

**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.**