



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Cargo and Billing System (CAB)

United States Transportation Command (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 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.

Public Law 100-562, Imported Vehicle Safety Compliance Act of 1988; 5 U.S.C. 5726, Storage Expenses, Household Goods and Personal Effects; 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, 19 U.S.C. 1498, Entry Under Regulations; 37 U.S.C. 406, Travel and Transportation Allowances, Dependents, Baggage and Household Effects; Federal Acquisition Regulation (FAR); Joint Federal Travel Regulation (JTR), Volumes I and II, DoD Directive 4500.9E, Transportation and Traffic Management; DOD Directive 5158.4, United States Transportation Command; DoD Instruction 4500.42, DoD Transportation Reservation and Ticketing Services; DoD Regulation 4140.1, DoD Materiel Management Regulation; DoD Regulation 4500.9, Defense Transportation Regulation; and DoD Regulation 4515.13-R, Air Transportation Eligibility 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 CAB supports Surface Distribution and Deployment Command's (SDDC) cargo and billing functions. This system enables SDDC to accurately bill Defense Transportation System (DTS) customers and pay commercial transportation providers for the movement of DoD surface cargo. PII data originates from other DoD information systems, which collects the service member's name and Social Security Number to create a unique Transportation Control Number (TCN).

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

Privacy risks associated with the PII collected include the potential of exposing social security numbers and last name. This information is protected with role based permissions to ensure that only authorized personnel can access the PII. Personal information is only disclosed to and used by authorized individuals who have a need to know this information to perform their duties.

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.

CAB receives PII via system interfaces, therefore, CAB has no contact (direct or indirect) with the individuals concerned. However, the originating system provides the individual the opportunity to object to the 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.

CAB receives PII via system interfaces, therefore, CAB has no contact (direct or indirect) with the individuals concerned. Originating systems provide banners to inform individuals of the authority to consent to PII collection. These 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, and the consequences 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.

- Privacy Act Statement**
- Other**
- Privacy Advisory**
- None**

Describe each applicable format.	<p>CAB receives PII via system interfaces, therefore, CAB has no contact with the individuals concerned. However, the originating systems provides the following Privacy Act Statements.</p> <p>The Global Air Transportation Execution System (GATES) Privacy Act (PA) statement: AUTHORITY: 10 U.S.C. 8013; EO 9397, 22 November 1943 PRINCIPAL PURPOSE: To apply for air travel. SSN is needed for positive ID. ROUTINE US(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.</p> <p>The Privacy Act statement used by Integrated Booking System: DD Fm 1299 - APPLICATION FOR SHIPMENT AND/OR STORAGE OF PERSONAL PROPERTY AUTHORITY: 37 USC 406, 5 USC 5726; and E.O. 9397. PRINCIPAL PURPOSE(S): Primarily used for evaluating requests submitted by Service members and eligible individuals for shipment and/or storage of personal property. Also used to prepare the Government bill of lading and other shipping documents (as applicable) to move the personal property. Used by the Finance Office for collection from the member in case goods to be shipped exceed Government entitlement limits.</p> <p>Transportation Financial Management System - MTMC (TFMS-M) collects PIIs using only a paper form, TFMS Form 417. The form states: "Completion of this form constitutes consent to use of Privacy Information for payment of payroll and entitlements. Failure to provide this information will result in inability of the organization to process payment. This information is collected under the authority of DoD Financial Management Regulations and will be protected in compliance with the Privacy Act of 1974, as amended."</p>
----------------------------------	--

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.