



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Travel Management Office Passport
Defense Travel Management Office

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

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.

5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence; 10 U.S.C. 135, Under Secretary of Defense (Comptroller); 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 37 U.S.C. 463, Programs of Compliance, Electronic Processing of Travel Claims; DoD Directive 4500.09E, Transportation and Traffic Management; DoD Directive 5100.87, Department of Defense Human Resources Activity (DoDHRA); DoD Instruction 5154.31, Commercial Travel Management; DoD Financial Management Regulation 7000.14-R, Vol. 9, Travel Policy; DoD 4500.9-R, Defense Transportation Regulation (DTR), Parts I-V; 41 C.F.R. 300-304, Federal Travel Regulation System; The Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members); The Joint Travel Regulation (Vol. 2) (Department of Defense Civilian Personnel); 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.

To establish a repository of DoD travel records consisting of travel booked within DTS as well as through commercial travel vendors in order to satisfy reporting requirements; to identify and notify travelers in potential distress due to natural or man-made disaster; to assist in the planning, budgeting, and allocation of resources for future DoD travel; to conduct oversight operations; to analyze travel, budgetary, or other trends; to detect fraud and abuse; to respond to authorized internal and external requests for data relating to DoD official travel and travel related services, including premium class travel. To provide website registered guests an online customer support site for submitting inquiries regarding commercial travel within the DoD, including assistance with DTS.

For DoD travelers, information from commercial travel booking systems and the Defense Travel System: name, Social Security Number (SSN), truncated SSN, gender, date of birth, dependent information (name, date of birth, and passport number), e-mail address, Service/Agency, organizational information, mailing address, home address, home, business, and cellular phone numbers, emergency contact information, duty station information, title/rank, civilian/military status information, travel preferences, frequent flyer information, passport information, DoD identification number, financial information to include government and/or personal charge card account numbers and expiration information, personal checking and/or savings account numbers, government accounting code/budget information, specific trip information to include travel itineraries (includes dates of travel) and reservations, trip record number, trip cost estimates, travel vouchers, travel-related receipts, travel document status information, travel budget information, commitment of travel funds, records of actual payment of travel funds, government travel charge card transactions, and supporting documentation.

For foreign national civilians on invitational travel orders: Foreign Identification Number or Individual Taxpayer Identification Number, name, date of birth, and passport information.

For registered website guests: name, phone number, e-mail address, duty station, rank, DoD identification number; if desiring travel alerts, cellular phone number and cellular phone provider; for issues related to the Defense Travel System, truncated SSN.

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

The unauthorized disclosure of information contained in this information system could lead to the identity theft of individuals whose records are stored in the system. Records are stored on secure military installations. Physical controls include use of visitor registers and identification badges, electronic key card access, and closed-circuit television monitoring. Technical controls including intrusion detection systems, secure socket layer encryption, firewalls, and virtual private networks protect the data in transit and at rest. Physical and electronic access is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their official duties. Usernames and passwords and Common Access Cards (CACs), in addition to role-based access controls are used to control access to the systems data. Procedures are in place to deter and detect browsing and unauthorized access including periodic security audits and monitoring of users' security practices. Backups are stored on encrypted media and secured off-site.

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.

-Services and Agencies responsible for individuals found to be in areas affected by natural disasters or threatening events.
-Services and agencies responsible for individuals suspected of fraud and abuse of travel services.
-Service/Agency Investigative Offices requesting data in support of investigation activities.

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.

For DTMO Passport help desk, users may elect not to register for an account. Individuals who do not register for an account may not receive help desk support, training, or travel planning information.

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

For the DTMO Passport data repository, data is collected from other systems (Defense Travel System (DTS), the Global Distribution System, Citi), not from the customer.

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.

Data within the information system is collected with no interaction with the customer. The information system contains PII records collected in other systems, thus the individual is presented with the privacy notices and user agreements of the original system of record. DTMO Passport is compliant with the uses contained in the original system of records notice.

DoD Travel Card users provide consent when signing the travel card application.

Users registering in the DTMO Passport for help desk support, training, or travel planning information consent to the use of their information in accordance with the website privacy policy by submitting their registration.

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

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

AUTHORITY: 5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence; 10 U.S.C. 135, Under Secretary of Defense (Comptroller); 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 37 U.S.C. 463, Programs of Compliance, Electronic Processing of Travel Claims; DoD Directive 4500.09E, Transportation and Traffic Management; DoD Directive 5100.87, Department of Defense Human Resources Activity (DoDHRA); DoD Instruction 5154.31, Commercial Travel Management; DoD Financial Management Regulation 7000.14-R, Vol. 9, Travel Policy; DoD 4500.9-R, Defense Transportation Regulation (DTR), Parts I-V; 41 C.F.R. 300-304, Federal Travel Regulation System; The Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members); The Joint Travel Regulation (Vol. 2) (Department of Defense Civilian Personnel); and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): To provide website registered users an online customer support site for submitting inquiries regarding commercial travel within the DoD, including assistance with the Defense Travel System. [add link to SORN when published.]

ROUTINE USE(S): The DoD Blanket Routine Uses found at <http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> may also apply to this collection.

DISCLOSURE: Voluntary. However, failure to provide requested information may limit DTMO's ability to provide travel assistance.

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.

