PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Defense Travel System

DoD Component Name:

Business Transformation Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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 125

☐ **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** **Enter UPI** 007-97-01-31-01-6312-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☐ **No**

d. Does the DoD information system or electronic collection have 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** **Enter Privacy Act SORN Identifier** T7334

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.

☐ **No**

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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. §§ 5701-5757, 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; 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 Financial Management Regulation 7000.14-R, Vol. 9, Travel Policies and Procedures; 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 provide a DoD-wide travel management process which will cover all official travel, from pre-travel arrangements to post-travel payments, to include the processing of official travel requests for DoD personnel, and other individuals who travel pursuant to DoD travel orders; to provide for the reimbursement of travel expenses incurred by individuals while traveling on official business; and to create a tracking system whereby DoD can monitor the authorization, obligation, and payment for such travel. Traveler's name, Social Security Number, gender, e-mail address, Service/Agency, organizational information, mailing address, home address, emergency contact information, duty station information, title/rank, civilian/military status information, travel preferences, frequent flyer information, passport information. Information in this system is obtained from the individual traveler, related voucher documents, Defense Accounting Offices (DAOs), and other DoD Components, government and/or personal charge card account numbers and expiration information, personal checking and/or savings account numbers, government accounting code/budget information, travel itineraries 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, and supporting documentation.

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

The risks are exposure of PII data to unauthorized personnel without a need to know. The risk is mitigated through a combination of technical and procedural controls. Technical controls within the system that limit the potential exposure of PII to unauthorized personnel include, but are not limited to use of public key enabled authentication, permission-, group- and organizationally-based access controls, encryption of data in transit and on backup tapes, and data masking. Procedural controls include, but are not limited to, procedures for properly storing, handling, and disposing of sensitive PII data.

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

All DOD components use DTS and have access to their own data stored within the system.

☐ **Other Federal Agencies.** Specify

☐ **State and Local Agencies.** Specify

☒ **Contractor** (enter name and describe the language in the contract that safeguards PII.) Specify

Northrop Grumman (prime contractor) and contractors supporting DTS user organizations.

☐ **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 the method by which individuals can object to the collection of PII.

Privacy notice presented to user prior to login states "DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and the claim for reimbursement. "

(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.

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

Once stored within the system, use of the data is controlled by the DTS application, not by the user.

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.

PRIVACY ACT

AUTHORITY: 5 U.S.C 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; 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 Directives 7000.14-R; and E.O. 9397 (SSN). PRINCIPAL PURPOSE(S): To obtain information for processing a request to travel at Government expense on official Department of Defense business and for processing a claim for reimbursement of authorized and legitimate expenses incurred as a result of such travel.

ROUTINE USE: For Federal and private entities providing travel services for purposes of arranging transportation at Government expense for official business.

DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and the claim for reimbursement.

DEPARTMENT OF DEFENSE: Department of the Army Narrative Statement on a New System of Records Under the Privacy Act of 1974.

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.