PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Travel System (DTS) - Defense Manpower Data Center (DMDC)

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

DTS provides a DoD-wide travel management system 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.

DTS includes a business intelligence tool and archive that provide a repository for reporting and archiving travel records and can be used to satisfy reporting and records management requirements. It is used to analyze travel and budgetary trends, respond to requests for data related to travel, and detect fraud and abuse.

DTS collects the following types of personal information: full name, Social Security Number (SSN), DoD Identification Number (DoDID), gender, date of birth, Passport information, mailing address, home address, emergency contact information, and personal email address. It collects employment information including Service/Agency, duty station information, title/rank, civilian/military status information, and work email address. It collects financial information including the government travel card number and expiration date, personal credit card number and expiration date, and personal checking and/or savings account numbers and bank routing information. And it collects travel information including frequent flyer information, 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, and supporting documentation.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected for identification verification for airline ticketing in compliance with Homeland Security regulations. Verification of bank account information for direct deposit of voucher and payment of travel card expenses. PII is also used to establish a repository of travel records which can be used to satisfy reporting requirements; 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; and to respond to authorized internal and external requests for data relating to DoD official travel and travel related services.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

If individuals object to the collection of their PII, then they should not enter the DTS system or accept the disclosure upon DTS login. They may request a manual itinerary generation to reduce the amount of PII that is collected, however, ultimately, if they choose to travel on DoD orders, they must allow the collection of PII. The privacy notice presented to the 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."

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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 have opportunity to consent before entering the site by clicking "accept" on the Privacy and Ethics Policy banner page. Once stored within the system, use of the data is controlled by the DTS application, not by the user.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

The following Privacy Act Statement is presented to the individual upon access the DTS login page. The statement is presented electronically on the web-based application.

PRIVACY ACT
AUTHORITY: 5 U.S.C. 57, Travel, Transportation, and Subsistence; DoD Directive 5100.87, Department of Defense Human Resources Activity; DoD Instruction 5154.31, Volume 3, Commercial Travel Management: Defense Travel System (DTS); DoD Financial Management Regulation 7000.14-R, Vol. 9, Defense Travel System Regulation, current edition; DoD Directive 4500.09E, Transportation and Traffic Management; DTR 4500.9-R, Defense Transportation Regulation, Parts I, Passenger Movement, II, Cargo Movement, III, Mobility, IV, Personal Property, V, Customs; 41 C.F.R. 300-304, The Federal Travel Regulation (FTR); Joint Federal Travel Regulations, Uniformed Service Members and DoD Civilian Employees; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): The purpose of DTS is to provide a DoD-wide travel management process which will cover all official travel, from pre-travel arrangements to post-travel payments. The system facilitates the processing of official travel requests for DoD personnel and other individuals who travel pursuant to DoD travel orders. DTS provides information to financial systems to provide the reimbursement of travel expenses incurred by individuals while traveling on official business. DTS includes a tracking and reporting system whereby DoD can monitor the authorization, obligation, and payment for such travel. The DTS pilot program evaluates more modern technology, common practices of the travel industry, and the feasibility of a commercial travel product to make DoD travel operations more efficient.

ROUTINE USE: To Federal and private entities providing travel services for purposes of arranging transportation and lodging for those individuals authorized to travel at government expense on official business. To the Internal Revenue Service to provide information concerning the pay of travel allowances which are subject to federal income tax. To banking establishments for the purpose of confirming billing or expense data. See the applicable system of records notice for a complete listing of routine uses: DMDC 28 DoD, Defense Travel System (DTS) located at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[ ] Within the DoD Component	Specify.	
[X] Other DoD Components	Specify.	All DOD components use DTS and have access to their own data stored within the system. Defense Travel Management Office (DTMO) also uses travel data metrics for inquiries and program management.
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	The DTS operations and maintenance contractors and DTS PMO support contractors comply with the requirements of OMB Memorandum M-06-16, Protection of Sensitive Agency Information, DoD Memorandum of June 23, 2006, DoD Guidance on Protecting PII, and DHRA Policy and Procedures When Personal Information is Lost, Stolen or Compromised. DTS contractors access information on an as-needed basis to troubleshoot system issues and respond to program inquiries.

☐ Other *(e.g., commercial providers, colleges).* Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☐ Databases
☒ Existing DoD Information Systems
☐ Commercial Systems
☐ Other Federal Information Systems

Information can be entered either by the user's service/agency (using the Defense Travel Administration (DTA) Maintenance functionality) or by the user (using the Self-Registration capability). DTS provides an import capability for some Services/Agencies where PII data can be electronically provided, DoD information system to DoD information system as in the case of the Air Reserve Orders Writing System (AROWS) and Navy Reserve Order Writing System (NROWS).

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Face-to-Face Contact
☐ Paper
☐ Fax
☐ Telephone Interview
☒ Information Sharing - System to System
☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DHRA 08 DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. 44 USC, Chapters 29, 31 and 33; 36 CFR 1220-1236, DoD 5015.02, and

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

The majority of the records will be destroyed 6 years after the final payment or cancellation. Records relating to a claim will be destroyed 6 years and 3 months after the claim is closed or court order is lifted. In the case of a waiver of a claim, the record will be destroyed 6 years and 3 months after the close of the fiscal year in which the waiver was approved. In the case of a claim for which the Government's right to collect was not extended, the record will be destroyed 10 years and 3 months after the year in which the Government's right to collect first accrued.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. 57, Travel, Transportation, and Subsistence; DoD Directive 5100.87, Department of Defense Human Resources Activity; DoD Instruction 5154.31, Volume 3, Commercial Travel Management: Defense Travel System (DTS); DoD Financial Management Regulation 7000.14-R, Vol. 9, Defense Travel System Regulation, current edition; DoD Directive 4500.09E, Transportation and Traffic Management; DTR 4500.9-R, Defense Transportation Regulation, Parts I, Passenger Movement, II, Cargo Movement, III, Mobility, IV, Personal Property, V, Customs; 41 C.F.R. 300-304, The Federal Travel Regulation (FTR); Joint Federal Travel Regulations, Uniformed Service Members and DoD Civilian Employees; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB Control Number: 0704-0577 Expiration Date: 09/30/2021

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☐ Citizenship	☒ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☒ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☒ Other ID Number
☒ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☐ Work E-mail Address	☒ If Other, enter the information in the box below	

Government travel credit card information, and personal bank account routing and account number, and other information which includes travel preferences such as frequent flyer information, TSA PreCheck number, etc.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Current memo on file is expired and currently up for renewal at this time. Exp 09/13/2020

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Use of the SSN within the DTS is covered by sections 2.c (4), (7), (8) and (11) acceptable uses described in DoDI 1000.30: "Interactions With Financial Institutions", "Federal Taxpayer Identification Number", "Computer Matching," and "Legacy System Interface". As the tax identification number for all travelers, the SSN, is required by the vendor in order to facilitate payment of the government travel charge card by Defense Finance and Accounting Service. In cases of investigations and audits, the SSN is also required to allow law enforcement and tax authorities to cross-reference and validate account numbers and user identifications in the system.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

There are no plans at this time to reduce the use of SSN in the current system as DTS interfaces with many older systems, removal of the SSN from the database and implementing a change of this magnitude adds substantial risk to the performance of each of these systems.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

Currently, none of the Service personnel systems have transitioned to the use of the DoD ID Number, although DTMO has encouraged such change. The only way to uniquely identify using the above named data source is to request and use the SSN.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically

conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [x] Cipher Locks
- [ ] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [ ] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Common Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [ ] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [ ] Least Privilege Access
- [ ] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [x] User Identification and Password
- [x] Virtual Private Network (VPN)
- [x] If Other, enter the information in the box below

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Records are stored in office buildings protected by security guards, closed circuit TV, controlled screening, use of visitor registers, electronic access, key cards, ID badges, and/or locks. Access to the systems data is controlled using intrusion detection systems, firewalls, a virtual private network, and DoD PKI certificates. Procedures are in place to deter and detect browsing and unauthorized access. To access the records, personnel are assigned role-based access and must complete two-factor authentication using a CAC credential and password/ PIN. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their official duties. Physical and electronic access are limited to persons responsible for servicing and authorized to use the record system. The backups of data are encrypted and secured. The program office conducts security audits and monitor security practices.