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 Management Office Passport / Commercial Travel Information Management

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

10/12/2018

Defense Travel Management Office

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.

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; identify and notify travelers in potential distress due to natural or man-made disaster; assist in the planning, budgeting, and allocation of resources for future DoD travel; conduct oversight operations; analyze travel, budgetary, or other trends; detect fraud and abuse; conduct surveys for the evaluation of program effectiveness, to calculate travel and housing allowances and provide insight into the gap between product/service delivery and customer expectations, and assist in understanding what drives customer satisfaction; and 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 repository records of DoD travelers, information from commercial travel booking systems and the Defense Travel System (DTS): name, Social Security Number (SSN), truncated SSN, gender, date of birth, 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 ID number, financial information to include government and/or personal charge card account numbers and expiration information, government travel charge card transactions, 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 and supporting documentation.

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

For repository records of dependents who are accompanying the DoD sponsor on travel: name, date of birth, and passport information.

For registered website guests: name, phone number, e-mail address; if affiliated with DoD, duty station, rank, DoD ID number; if desiring travel alerts, cellular phone number and cellular phone provider; if requiring assistance with DTS, last four of the SSN.

Employment information includes duty station information, title/rank, civilian/military status information; Spouse and child information includes name, date of birth, passport number; Other ID number includes DoD ID Number, Passport number, Foreign Identification Number, Individual Taxpayer Identification Number, Frequent Flyer Number; Financial information includes government and/or personal charge card

account numbers and expiration information, personal checking and/or savings account numbers, government accounting code/budget information, government travel charge card transactions; Other includes 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, 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)*

Verification, identification, authentication, data matching, and mission-related use.

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.

For the Commercial Travel Information Management data repository, PII data is collected from other systems (Defense Travel System (DTS), the Global Distribution System, Government Travel Credit Card vendor). Users are subject to the objection capabilities of the originating system.

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

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.

For the Commercial Travel Information Management data repository, PII data is collected from other systems (Defense Travel System (DTS), the Global Distribution System, Government Travel Credit Card vendor), thus the individual is presented with the privacy notices and user agreements of the originating systems. For example, Government Travel Charge Card users provide consent to the use of their information when signing the travel card application. DTMO Passport is compliant with the uses contained in the original system notices.

Users registering on the DTMO Passport website 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.

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

PAS Displayed Upon System Registration:
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; DoD Instruction 1100.13, Surveys of DoD Personnel; The Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members); The Joint Travel Regulation (Vol. 2) (Department of Defense Civilian Personnel); 41 C.F.R. 300-304, Federal Travel Regulation System; 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.

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 522a(b) of the Privacy Act of 1974, as amended.

To Federal and private entities providing travel services for purposes of arranging transportation at Government expense for official business. Additional routine uses are listed in the applicable System of Records Notice, DHRA 14 DoD, Commercial Travel Information Management System at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570773/dhra-14-dod/

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

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.	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.
[X] Other Federal Agencies	Specify.	Ad hoc travel reports to other DoD components for reasons that fall within the uses established in the CTIM SORN
[ ] 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.	CKA, LLC - FAR privacy clauses 52.224-1, Privacy Act Notification and 52.224-2, Privacy Act are included in the contract. iJet - FAR privacy clause 52.224-2, Privacy Act is included in the contract.
[ ] 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)*

- [X] Individuals
- [X] Existing DoD Information Systems
- [X] Other Federal Information Systems
- [ ] Databases
- [X] Commercial Systems

Defense Travel System General Services Administration data repository, commercial systems (Global Distribution System, Citi)

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

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

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DHRA 14 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. GRS 9, Item 3a (N1-GRS-91-3, Item 3a.)

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

(3) Retention Instructions.

Destruction: Temporary, Cut off annually, Destroy 6 years after cut off.

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. 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; DoD Instruction 1100.13, Surveys of DoD Personnel; The Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members); The Joint Travel Regulation (Vol. 2) (Department of Defense Civilian Personnel); 41 C.F.R. 300-304, Federal Travel Regulation System; 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.

0704-0577, "Defense Travel System," September 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	

For repository records of DoD travelers, information from commercial travel booking systems and the Defense Travel System (DTS): travel preferences, frequent flyer information, passport 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 and supporting documentation.

For repository records of foreign national civilians on invitational travel orders: Foreign Identification (ID) Number or Individual Taxpayer ID Number.

Employment information includes duty station information, title/rank, civilian/military status information; Spouse and child information includes name, date of birth, passport number; Other ID number includes DoD ID Number, Passport number, Foreign Identification Number, Individual Taxpayer Identification Number, Frequent Flyer Number; Financial information includes government and/or personal charge card account numbers and expiration information, personal checking and/or savings account numbers, government accounting code/ budget information, government travel charge card transactions; Other includes 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, and supporting documentation.

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.

SSN Justification Memo from 2014 is in place. Latest version pending approval.

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

Legacy System Interface
Interaction With Financial Institutions

(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".

DTMO's system does not display SSN or partial SSN on any publicly accessible content. DTMO will migrate away from SSN usage once the feeding systems are able to do so.

(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

SSN use in this system can only be accomplished if the feeding systems migrate to an alternate identifier. To-date, no such plan has been conveyed to the DTMO from any of the applicable source systems.

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)*

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

Records are stored on secure military installations

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

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

Visitor registries

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

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

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

The additional measures/safeguards that are put in place to address privacy risks for this information system is secured with the use of key cards, security guards, closed circuit TV (CCTV) identification badges safes, backups will be secured off-site, encryption of backups, methods to ensure only authorized personnel access to PII, periodic security audits, regular monitoring of users' security practices, visitor registries, encryption of data at rest, firewalls, role-based access controls, virtual private network (VPN), common access card (CAC, encryption of data in transit, intrusion detection system (IDS) DoD Public Key Infrastructure Certificates, external certificate authority certificates, least privilege access, and user identification and password.