DEPARTMENT OF DEFENSE **BILLING CODE:**

Office of the Secretary

[Docket ID: DoD-2018-OS-XXXX

Privacy Act of 1974; System of Records

AGENCY: Defense Manpower Data Center, DoD.

ACTION: Notice of a Modified System of Records

SUMMARY: The Defense Manpower Data Center is modifying a system of records, Defense Travel System, DMDC 28 DoD. The Defense Travel System (DTS) is the standard Department of Defense (DoD) travel system used for processing and managing unclassified temporary duty travel. DTS streamlines the DoD travel processes. It provides for the procurement of commercial travel services through the DTS web portal that will book travel reservations, compute the costs associated with each trip, reconcile cost, disburse payment, and archive each travel record in accordance with DoD requirements.

DATES: Comments will be accepted on or before [**INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria,

VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

SUPPLEMENTARY INFORMATION: The national defense strategy of the United States requires a strong Defense Transportation System (DTS), operating within a national transportation system that is fully responsive and globally capable of meeting personnel and materiel movement requirements of the Department of Defense across the range of military operations. This strategy requires that an optimum mix be achieved that matches defense requirements with the various modes and methods of transportation, both military and commercial. It is DoD policy that the DTS is the single online travel system used by the DoD. The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at http://dpcld.defense.gov/.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on INSERT DATE, to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and

Budget (OMB) pursuant to Section 6 to OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated:

Aaron Siegel
Alternate OSD Federal Register Liaison Officer, Department of Defense

SYSTEM NAME AND NUMBER: Defense Travel System (DTS), DMDC 28 DoD

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Operational DTS is located at the Central Data Center 1, Quality Technology Services (QTS), 1506 Moran Road, Dulles, VA 20166-9306 with the COOP site at the Central Data Center 2, Quality Technology Services (QTS), 1175 N. Main Street, Harrisonburg, VA 22802-4630.

The DTS Archive is located at Defense Manpower Data Center, DoD Center, Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

The DTS Modernization Effort is located in the Concur cloud platform, a commercial entity, Concur Technologies, Inc.,700 Central Expressway South, Suite 230, Allen, Texas 75013 -8104.

SYSTEM MANAGER(S): Deputy Director, Defense Travel Management Office, 4800 Mark Center Drive, Suite 04J25-01, Alexandria, VA 22350-6000; email: dodhra.dodc-mb.dmdc.mbx.webmaster@mail.mil.

For archived records: Deputy Director, Defense Travel System Archive, Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 57, Travel, Transportation, and Subsistence; Department of Defense (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.

PURPOSE(S) OF THE SYSTEM: 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 business intelligence tool and archives provide a repository for reporting and archiving travel records which can be used to satisfy reporting and records management requirements. It assists 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 provides the tool to respond to authorized internal and external requests for data relating to DoD official travel and travel-related services.

The DTS modernization effort 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. The scope of the effort starts small and will expand over time to include more functionality and different types of users throughout DoD.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DoD civilian personnel; active, former, and retired military members; Reserve and National Guard

personnel; academy nominees, applicants, and cadets; dependents of military personnel; and all other individuals in receipt of DoD travel orders.

CATEGORIES OF RECORDS IN THE SYSTEM: DTS collects the following types of personal information: full name, Social Security Number (SSN), DoD Identification Number (DoD ID Number), gender, date of birth, Passport information, mailing address, home address, emergency contact information, and personal email address. Employment information including Service/Agency, duty station information, title/rank, civilian/military status information, and work email address. Financial information including the government travel card number and expiration date, personal credit card number and expiration date, personal checking and/or savings account numbers and bank routing information. 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.

RECORD SOURCE CATEGORIES: The individual traveler, authorized DoD personnel, and DoD information systems via electronic import such as the Air Reserve Orders Writing System (AROWS) and Navy Reserve Order Writing System (NROWS).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. 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.

b. To the Internal Revenue Service to provide information concerning the pay of travel allowances which are subject to federal income tax.

c. To banking establishments for the purpose of confirming billing or expense data.

d. To contractors responsible for performing or working on contract for the DoD when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DoD officers and employees.

e. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

f. To a federal agency, in response to its request in connection with an investigation of an employee, service member, or other authorized individualto the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

g. To the Office of Personnel Management concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

h. To the Department of Justice for Litigation for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

i. To the National Archives and Records Administration for records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

j. To the Merit Systems Protection Board, including the Office of the Special Counsel, for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; and administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

k. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

l. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to

prevent, minimize, or remedy such harm.

m. To a Federal, State, local, tribal, territorial, foreign governmental and/or multinational agency, either in response to its request or upon the initiative of the Component, or maintained by a Component consisting of, or relating to, terrorism information (6 U.S.C. 485(a)(4)), homeland security information (6 U.S.C. 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment, November 22, 2006) may be disclosed for purposes of sharing such information as is necessary and relevant for the agencies to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) and Executive Order 13388 (October 25, 2005).

n. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

o. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems,

programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Travel authorization and voucher records for DoD employees are retrieved by the DoD Component, name, and/or partial or full SSN. For foreign nationals, records can be retrieved using the full name and DoD component. For employees' dependents, records can be retrieved using the host employee's component, name, and SSN. For the modernization effort (which only includes a small subset of Federal Government employees) the data is retrieved by DoD ID Number and name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records are retained and disposed of consistent with the National Archives and Records Administration approved records disposition schedules. 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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: 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 system's 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.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system of records should address written requests to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington DC 20301-1155.

Requests must include the name and number of this system of records notice in addition to the individual's full name, SSN (if applicable), office or organization where assigned when trip was taken, and dates of travel. The request must be signed by the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:
If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executied on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the System Manager.

NOTIFICATION PROCEDURE: Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the Deputy Director, Defense Travel Management Office, 4800 Mark Center Drive, Suite 04J25-01, Alexandria, VA 22350-6000 or (for archived records) the Deputy Director, Defense Travel System/Management Information System, Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771.

Individuals should provide their full name, office or organization where assigned when trip was taken, and dates of travel. In the case of legal claims or duplicate names, an individual's SSN (last 4 digits or full number, depending on the scenario) may be required.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executied on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: March 24, 2010, 75 FR 14142.