



**BILLING CODE: 5001-06**

**DEPARTMENT OF DEFENSE**

**Office of the Secretary**

**[Docket ID: DOD-2018-OS-0056]**

**Privacy Act of 1974; System of Records**

**AGENCY:** Office of the Secretary of Defense, DoD.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** The Office of the Secretary of Defense (OSD) proposes to modify a system of records titled, "Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) Records, DMDC 18 DoD." SPOT-ES is used at installations to manage, track, account for, monitor and report on contracts, companies, and contractor employees supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require contractor support. This modification enables DoD to comply with an existing treaty which requires tracking of contractor employees' collocated dependents. The modification also reflects changes to the the following sections: system manager, authorities, purpose, categories of individuals, categories of records, routine uses, safeguards, record access procedures, notification procedures, and exemptions.

**DATES:** Comments will be accepted on or before [**INSERT DATE 30 DAYS AFTER 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 for 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:** Ms. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, DC 20311-1155, or by phone at (571) 372-0478.

**SUPPLEMENTARY INFORMATION:** The OSD proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. The DoD uses the system of records at installations to manage, track, account for, monitor and report on contracts, companies, and contractor employees supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require contractor support. As a part of maintaining DoD installations in other nations, the Department must comply with existing treaties between the United States and host nations. This modification ensures DoD complies with an existing treaty between the U.S. and Japan by collecting additional information on the co-located dependents of contractor employees. This

modification updates the following sections: category of individuals, category of records, the authority for the maintenance, and the purpose and also reflects the reformatting of the notice to ensure compliance with Office of Management and Budget Circular Number A-108, “Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.”

The OSD 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://dpclld.defense.gov/>.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on August 3, 2018, 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: August 15, 2018.

**Aaron T. Siegel,**

*Alternate OSD Federal Register Liaison Officer,*

*Department of Defense.*

**SYSTEM NAME AND NUMBER:** Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) Records, DMDC 18 DoD.

**SECURITY CLASSIFICATION:** Unclassified and Classified. This system is comprised of two databases: an unclassified database that serves as the primary repository of contract and contractor personnel records and a classified database containing only classified records [related to a specific category of individuals].

**SYSTEM LOCATION:** Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6784.

Stand-alone Joint Asset Movement Management System (JAMMS) machines are deployed as needed to locations within and outside the United States. A list of current JAMMS locations are available upon written request to the system manager.

**SYSTEM MANAGER(S):** Director, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000. Email: dodhra.dodc-mb.dmdc.mbx.webmaster@mail.mil.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 10 U.S.C. 2302 note, Contractors Performing Private Security Functions in Areas of Combat Operations or Other Significant Military Operations; Treaty of Mutual Cooperation and Security Between the United States of America and Japan, January 19, 1960; Department of Defense (DoD) Directive (DoDD) 1404.10, DoD Civilian Expeditionary Workforce; DoDD 3020.49, Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution; DoD Instruction (DoDI) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 3020.41, Operational Contract Support (OCS); DoDI 3020.50, Private Security Contractors (PSCs) Operating in Contingency

Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises; DoDI 6490.03, Deployment Health; and E.O. 9397 (SSN), as amended.

**PURPOSE(S) OF THE SYSTEM:** The Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) allows federal agencies and Combatant Commanders to plan, manage, track, account for, monitor and report on contracts, companies, and contractor employees supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require contractor support within and outside the United States. Authorized dependents may also be accounted for in designated locations as part of the sponsor's record. SPOT is a web-based system in the SPOT-ES providing a repository of military, Government civilian and contractor personnel, and contract information for DoD, Department of State (DOS), United States Agency for International Development (USAID), other federal agencies, and Combatant Commanders to centrally manage their supporting, deploying, deployed, and redeploying assets via a single authoritative source for up-to-date visibility of personnel assets and contract capabilities. The system is also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

The Joint Asset Movement Management System (JAMMS) is a stand-alone application in the SPOT-ES that scans identity credentials (primarily held by military, Government civilians, and contractors) at key decentralized locations. The Total Operational Picture Support System (TOPSS) is a web-based application in the SPOT-ES that integrates information from SPOT and JAMMS to provide trend analysis, widgets and reports from different views based on the user access level and parameters selected to support DoD, DOS, USAID, other federal agencies, and Combatant Commanders' requirements.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** DoD military personnel and civilian personnel supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, events, and other activities that require support within and outside the U.S.

DoD contractor personnel supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require contractor support within and outside the U.S.

DOS and USAID contractor personnel supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations both within and outside of the U.S., and during other missions or scenarios.

DOS and USAID civilian employees supporting contingency operations led by DoD or the DOS Office of Security Cooperation outside of the U.S. Government civilian and contractor personnel of other agencies.

Personnel of agencies such as the Department of Interior, Department of Homeland Security, Department of Treasury, Department of Justice, Department of Health and Human Services, Environmental Protection Agency, Department of Transportation, Department of Energy, and General Services Administration that may use the system to account for their personnel when supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, exercises, events, and other activities within and outside the U.S.

The system may also include civilians in private sector organizations and private citizens, including first responders, who are in the vicinity, are supporting, or are impacted

by operations, e.g., contingency, humanitarian assistance, or disaster relief, and transit through a location where a JAMMS workstation is deployed.

**CATEGORIES OF RECORDS IN THE SYSTEM:** For contractor personnel: full name; blood type; Social Security Number (SSN); DoD Identification (ID) Number; Federal/foreign ID number or Government-issued ID number, e.g., passport and/or visa number; category of person; home, office, and deployed telephone numbers, address, and email; emergency contact name and telephone number; next of kin name, phone number and address; duty location and duty station; travel authorization documentation, i.e., Letters of Authorization (LOAs); air travel itineraries, movements in the area of operations; in-theater and Government authority points of contact; security clearance information; and predeployment processing information, including completed training certifications.

For contractors deployed to Japan these additional items will be captured: Status of Forces Agreement (SOFA) status and expiration date; affirmation that the contractor possesses a residency permit or residency visa for Japan; number of dependents, and Japan-specific authorized government services.

For dependents authorized to accompany contractor personnel in Japan: full name, date of birth, family relationship, sponsoring family member full name, passport number, and passport country.

For DoD military and civilian personnel: full name, SSN, DoD ID Number, category of person (civilian or military), and movements in the area of operations.

For other federal agency personnel: full name, SSN, Government-issued ID number (e.g., passport and/or visa number), category of person, and movements in the area of operations.

For non-Government personnel: full name, Government-issued ID number (e.g., passport and/or visa number), and movements in the area of operations.

For contractor personnel: contract information data: contract number, task order number, contractor company name, contract capabilities, contract/task order period of performance, theater business clearance, company contact name, office address and phone number. Equipment and weapons data: contractor owned/contractor operated equipment in designated areas, type of equipment (roll-on/roll-off, self-propelled, containerized), authorized weapons assigned to specific contractor employees, contract number, contractor company name, and other official deployment-related information, e.g., types of training received.

**RECORD SOURCE CATEGORIES:** Individual's employer (military, Government civilians and contractor personnel), Defense Enrollment Eligibility Reporting System (DEERS), and federal entities supporting contingency, humanitarian assistance, peacekeeping, and disaster relief operations.

**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, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- a. To DOS and USAID to account for their Government civilian and contractor personnel

supporting operations outside of the U.S., and to determine status of processing and deployment documentation, contracts, weapons and equipment, current and historical locations, company or organization where an individual is employed, and contact information.

b. To Federal agencies associated with the categories of individuals covered by the system to account for their Government civilian and contractor personnel supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require support within and outside the U.S.

c. To contractor companies to account for their employees supporting contingency operations, humanitarian assistance operations, peace operations, disaster relief operations, military exercises, events, and other activities that require contractor support within and outside the U.S.

d. To applicable private sector organizations to account for their personnel located in an operational area.

e. To applicable facilities managers where JAMMS are deployed to account for Government services consumed and depict usage trends.

f. 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.

g. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

h. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative

body or official, when the DoD or other agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

- i. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
- j. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- k. 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.
- l. 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:** Within SPOT-ES, records are retrieved by full name, SSN, DoD Identification Number, or federal/foreign ID number.

Within JAMMS, records may be retrieved by last name at the specific machine used at a location within specified start and ending dates.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** Permanent. Close all files upon end of individual's deployment. Transfer to the National Archives and Records Administration when 25 years old.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** Electronic records in SPOT and TOPSS are maintained in a Government-controlled area accessible only to authorized personnel. Entry to these areas is restricted to those personnel with a valid requirement and authorization to enter. Physical entry is restricted by the use of lock, guards, and administrative procedures. Physical and electronic access is restricted to designated individuals having a need-to-know in the performance of official duties. Access to personal information is further restricted by the use of Public Key Infrastructure or login/password authorization. Information is accessible only by authorized personnel with appropriate clearance/access in the performance of their duties. For JAMMS, physical and electronic access is restricted to designated individuals having a need-to-know in the performance of official duties. Access to personal information is further restricted by the use of login/password authorization or may use two-factor authentication with CAC and PIN.

Physical entry is restricted to authorized personnel. Data transferred to SPOT-ES are encrypted.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to information about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act, Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, D.C. 20301-1155. Foreign nationals seeking access to their records must submit requests under the Freedom of Information Act at the above address.

Signed, written requests should contain the individual's full name, last four digits of the SSN, DoD ID Number or federal/foreign ID number, current address, telephone number, when and where they were assigned during the named operation or event, and the name and number of this system of records notice.

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. Executed 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 contained 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 should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6784.

Signed, written requests should contain the individual's full name, last four digits of the SSN, DoD Identification Number or federal/foreign ID number, current address, telephone number, and when and where they were assigned during the named operation or event.

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. Executed on (date). (Signature).'

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** The Department of Defense is exempting records maintained in DMDC 18 DoD, from subsection (d) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(1). Such information has been determined to be classified under criteria established by an Executive Order in the interest of national defense or foreign policy and is properly classified pursuant to such Executive Order. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c)

and (e) and published in 32 CFR part 311. For additional information contact the system manager.

**HISTORY:** May 26, 2015, 80 FR 30057; October 24, 2013, 78 FR 63455; March 18, 2010, 75 FR 13103.

[FR Doc. 2018-17955 Filed: 8/20/2018 8:45 am; Publication Date: 8/21/2018]