Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0056]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to alter a System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to alter a system of records, DMDC 18 DoD, entitled "Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) Records." The Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) allows federal agencies and Combatant Commanders the ability to plan, manage, track, account for, and 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 U.S.

DATES: Comments will be accepted on or before [**INSERT DATE 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 Deputy Chief Management Officer, Directorate for Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

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. Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Service, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0461.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), 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 and Civil Liberties Division website at http://dpcld.defense.gov/.

The proposed system report, as required by U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on May 20, 2015, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: May 20, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

DMDC 18 DoD

System name:

Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) Records (October 24, 2013, 78 FR 63455).

Changes:

* * * * *

System location:

Delete entry and replace with "Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

Stand-alone Joint Asset Movement Management System (JAMMS) machines are deployed as needed to locations within and outside the U.S. A list of current JAMMS locations can be provided upon written request to the system manager."

Categories of individuals covered by the system:

Delete entry and replace with "Department of Defense (DoD) military personnel and civilian employees 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.

Department of State (DOS) and United States Agency for International Development (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 Federal Agencies, e.g. 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 which 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.

Civilian 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:
Delete entry and replace with "Individual profile data: For contractor personnel, full name; blood type; Social Security Number (SSN); DoD Identification Number; Federal/foreign ID number or Government-issued ID number, e.g. passport and/or visa number; category of person (contractor); home, office, and deployed telephone numbers; home and deployed address; home, office, and deployed e-mail addresses; 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, and movements in the area of operations; in-theater and Government authority points of contact; and security clearance

information and pre-deployment processing information, including completed training certifications.

Contractor personnel performing private security functions: Type of media used to collect identity and the document ID. Authorized weapons and equipment, and other official deployment-related information, e.g. types of training received.

Contract information data:
Contract number, contractor company name, contract capabilities, contract value, contract/task order period of performance, theater business clearance, and company contact name, office address and phone number.

For DoD military and civilian personnel: full name, SSN, DoD Identification 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 (Federal civilian), 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."

Authority for maintenance of the system:
Delete entry and replace with "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; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Directive 1404.10, DoD Civilian Expeditionary Workforce; DoD Directive 3020.49, Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution; DoD Instruction 3020.41, Operational Contract Support (OCS); DoD Instruction 3020.50, Private Security Contractors (PSCs) Operating in Contingency Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises; DoD Instruction 6490.03, Deployment Health; and E.O. 9397 (SSN), as amended."

Purpose(s):

Delete entry and replace with “The Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES) allows federal agencies and Combatant Commanders the ability to plan, manage, track, account for, and 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 U.S.

The SPOT is a web-based system providing a repository of military, Government civilian and contractor personnel, and contract information for DoD, DOS, 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. Used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

JAMMS is a stand-alone application that scans identity credentials (primarily held by military, Government civilians, and contractors) at key decentralized locations,

e.g. dining facilities, billeting, central issue facilities, and aerial ports of debarkation. Also used as a management tool for statistical, tracking, reporting, evaluating program effectiveness, and conducting research.

The Total Operational Picture Support System (TOPSS) is a web-based application 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."

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Delete entry and replace with "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:

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.

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.

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.

To applicable civilian organizations to account for their personnel located in an operational area.

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

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice 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.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the

suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx"

* * * * *

Retrievability:
Delete entry and replace with "Within SPOT: Full name, SSN, DoD Identification Number, or Federal/foreign ID number.

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

Safeguards:
Delete entry and replace with "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. Once access is gained, the system is set with an automatic timeout period to reduce the opportunity for unauthorized access.

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. Computers running the JAMMS software are located on Government installations where physical entry is restricted to authorized personnel. Each machine is physically secured with a combination lock and cable. While the computer is active, the view screen is oriented away from the cardholder, and access is controlled

by an attendant on duty. While the data is at rest and when data is transferred to SPOT, the records are encrypted. Daily exports from JAMMS are uploaded, via encrypted file transfer, to SPOT as the mandated repository of information on contingency contract and contractor information."

* * * * *

[FR Doc. 2015-12629 Filed: 5/22/2015 08:45 am; Publication Date: 5/26/2015]