PRIVACY IMPACT ASSESSMENT (PIA)

For the

Synchronized Predeployment and Operational Tracker Enterprise Suite (SPOT-ES)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	6501
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI 007-97-01-04-02-1929-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 18 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. 16 April 2013

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number 0704-0460

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

10 U.S.C. 2302, note, Contracts in Iraq and Afghanistan and Private Security Contracts in Areas of Other Significant Military Operations; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology and Logistics; DoD Instruction 3020.41, Operational Contract Support (OCS); DoD Directive 3020.49, Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution; DoD Instruction 3020.50, Private Security Contractors (PSCs) Operating in Contingency Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises; DoD Directive 1404.10, DoD Civilian Expeditionary Workforce; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 6490.3, Deployment Health; DoD Implementation Guidance for SPOT, Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (OUSD (ATL)) Memo on Acquisition Support Center Deployment Cell, and E. O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

The Synchronized Predeployment and Operational Tracker (SPOT) allows federal agencies and Combatant Commanders the ability to plan, manage, track, account for, monitor and report on contracts, companies and contractor employees during planning, operation and drawdown of any contingency, peacekeeping, humanitarian or disaster-recovery operation both within and outside of the U.S. SPOT is a web-based system providing a repository of military, Government civilian and contractor personnel and contract information for DoD, DoS, USAID and other Federal Agencies and Combatant Commanders to centrally manage their deploying, deployed and redeploying assets via a single authoritative source for up-to-date visibility of personnel assets and contract capabilities. Also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.
The Total Operational Picture Support System (TOPSS) web-based application integrates the information in SPOT to provide trend analysis, widgets and reports from different views based on the user access level and parameters they select to support DoD, DoS, USAID, other Federal Agencies and theater commander requirements.

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

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

SPOT data is stored on a DoD-accredited infrastructure with associated operational information systems security protection in place. Protections are in place against physical, behavioral, environmental and software threats. Users require a verified software certificate (e.g., CAC) or sponsored login and password to access SPOT, thus minimizing the risk of unauthorized disclosure. In addition, SPOT contains role-based security so that the information provided to an authorized user is limited to that which is necessary for the task to be performed. Further restrictions within SPOT limit individuals based on their association with a specific contractor company or government organization.

Risk is mitigated in the SPOT ES products through least privilege. Least privilege limits information access to each system user to the minimum essential to perform official duties and no more. Least privilege is managed by system access control and by a job description and role assignment matrix. Risk is also mitigated by the use of FIPS 140-2 validated encryption, defense-in-depth devices such as Army- approved demilitarized zones (DMZs), intrusion detection systems / firewalls / routers, and finally physical security.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☒ **Other DoD Components.**

Specify. All Military Components

☒ **Other Federal Agencies.**

Specify. Department of State; U.S. Agency for International Development (USAID); 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 may use the system to account for their Government civilian and contractor personnel when supporting contingency, humanitarian, peacekeeping and disaster relief operations both within and outside of the U.S.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Contractor companies account for their employees during contingency, humanitarian, peacekeeping and disaster relief operations both within and outside of the United States.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Applicable civilian organizations, e.g. United Services Organization (USO), to account for personnel located in a contingency area.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

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

Data collection on contractors is a condition of their contract when DFARS 225.252-7040 is incorporated per DoD direction. Persons who choose not to have the data collected will not be entitled to DoD employment opportunities which require this data to be collected.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **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.

Information in SPOT-ES is not collected from the individual themselves. The information is input by the individual's employer. Thus, the individual is not given the opportunity to consent to the specific uses within the SPOT-ES.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

Data in SPOT-ES is not being collected directly from the individual, rather the information is input by the individual's employer. .

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.