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 UPI = 007-97-01-04-02-1929-00 UII = 007-000001929

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.

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	31 August 2016

☐ **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. 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 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 Instruction 6490.03, Deployment Health; 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.

● Privacy Act information collected is a condition of employment on DoD contracts whenever DFARS Clause 252.225-7040 is incorporated.
● The SPOT-ES Program provides two web-based applications and a deployable workstation application. Together, they provide federal agencies and Combatant Commanders with 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 United States.
● The Synchronized Predeployment and Operational Tracker (SPOT) is the central data repository of contract and contractor information for DoD, DoS and USAID. Other federal agencies also use SPOT as the authoritative source for this type of information. SPOT provides a standardized front-end user interface for companies to enter individual records along with logistics, operations, deployment, contract, and contact information. SPOT contains a work-flow process that generates a digitally signed Letters of Authorization (LOA), employs interfaces with other authoritative data sources for person and contract data, and provides up-to-date visibility of contractors, contractor assets and capabilities. Personal information collected and reported includes: first name, last name, middle name, social security number, DoD ID Number, date of birth, and gender.
● The Joint Asset Movement Management System (JAMMS) operates as a stand-alone workstation consisting of a laptop with scanner that is deployed to a high contractor density service points, e.g., Dining Facilities (DFAC) or Aerial Ports of Debarkation (APOD). JAMMS scans identity credentials (e.g., Common Access Card (CAC) and LOA), to collect person, date-time and location data. These scanned transactions are transferred daily to the SPOT database which appends the collected data to the appropriate individual's record. CAC scans are processed multiple times each day using the SPOT web service with DEERS. The DoD ID Number retrieved from the CAC is used to pull back the first name, last name, middle name, social security number, date of birth, and gender of the scanned individual. When information cannot be associated with an existing SPOT record, SPOT uses the data retrieved from DEERS to build a mini-record of a unique individual to which the associated scanned dates & locations are appended.
● The Total Operational Picture Support System (TOPSS) uses the information stored in SPOT to provide business intelligence, a common operating picture, and a reporting tool for Government users and certain contractors directly supporting Government offices. TOPSS aggregates data from SPOT to build a single virtual entity using advanced analytics to produce widgets, standard and ad hoc reports, customizable geospatial mapping of data points and trend analysis. TOPSS contains the same PII information (first name, last name, middle name, social security number, DoD ID, date of birth, and gender) as does SPOT.

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

● SPOT-ES data contains personally identifiable information (PII) and individual records are able to be retrieved by person-unique identifiers. There is a risk that the SPOT-ES systems may be targeted for unauthorized intrusion or hacking. These risks are addressed by administrative, physical and technical safeguards as described below.
● SPOT-ES data is stored on a DoD-accredited infrastructure with associated security protection for operational information technology (IT) systems. Protections are in place against physical, behavioral, environmental, cyber and software threats. Users require a verified software certificate (e.g., CAC) to access SPOT, thus minimizing the risk of unauthorized disclosure. A small number of users who cannot qualify for PIV-compliant credentials have sponsored login and password access. SPOT contains role-based security so 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.
● SPOT-ES uses a multi-tiered cybersecurity risk management process in accordance with DoDI 8500.01 & DoDI 8500.2. Risk is mitigated in the SPOT-ES products through least privilege. Least privilege limits information access for each system user to the minimum essential to perform official duties and no more. Least privilege is managed by system attribute based access control (ABAC) in accordance with the user's

specific job description and role assignment matrix. Encryption Wizard is used to safeguard information in reports prior to customer distribution. 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 physical security.

● SPOT-ES has an approved justification to use Social Security Numbers (SSN) for computer matching and legacy system interfaces per DoDI 1000.30. The SSN has been removed from places where it is not needed for these two justified uses. To further protect privacy information, the SSN has been replaced with the DoD ID Number wherever possible.

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 DMDC Systems.

☒ **Other DoD Components.**

Specify. All Military Components and Combatant Commanders

☒ **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; General Services Administration and other federal agencies 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. Law Enforcement Agencies as approved by the Program Manager.

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

Specify.

● Development Contractor
- ID03150053 DMDC SPOT-ES PWS.
- 4.4.3 The Contractor shall focus on interoperability and interface requirements and the associated security and privacy issues when interfacing / interoperating with federated environments.
- 6.9 Security: The Contractor shall:
-- 6.9.2 Comply with:
DoD Instruction (DoDI) 8500.1, Cybersecurity
The Privacy Act (5 U.S.C. 552a)
DoD 5400.11-R, and DoD Directive 5400.11, DoD Privacy Program
DoD 6025.18-R, DoD Health Information Privacy Regulation
DoD 5200.2-R, Personnel Security Program
HSPD-12, Homeland Security Presidential Directive.
-- 6.9.3 Comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, ... shall obtain CAC or PIV ready status prior to reporting for work. At a minimum, all Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check), two forms of identity proofed identification (I-9 document), and submit a National Agency Check and Law Credit (NACLAC) vetting package for processing.
-- 6.9.5 Immediately report the discovery of any Privacy breach first to the DMDC CIO/ Privacy Office and secondly to the COR.

-- 6.9.6 Perform off-site work with Personally Identifiable Information (PII) only on systems and platform information technology systems (PIT) that meet Risk Management Framework (RMF) (formerly Defense Information Assurance Certification and Accreditation Process (DIACAP)) for DoD Information Technology (IT) requirements. Systems must have and maintain an Authority to Operate (ATO).

● Customer Contractors
- DFARS 252.225-7040, Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States - requires all contractor personnel to comply with United States regulations, directives, instructions, policies, and procedures.
- Privacy Act of 1974 (5 U.S.C. 552a) - included in all contracts and data access responsibilities are published on system websites used by contractors.
- U.S. Citizenship and Immigration Services (USCIS) Form I-9 - each employee must complete OMB No. 1615-0047, Employment. Eligibility Verification.
- SPOT and TOPSS both present the 'Acknowledgment of Responsibilities of Receiving and Maintaining Privacy Act Data' each time a user logs onto SPOT and requires user's active selection of the 'I Consent' icon before allowing them to proceed with access to the application.

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

Specify. Applicable civilian organizations, e.g., United Services Organization (USO), to account for personnel located in a contingency, peacekeeping, humanitarian relief or disaster response / recovery 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 directly from the individual. The SPOT records are input by the individual's employing company. Use of the PII is required by laws and regulations that necessitate the use of the Privacy Act information for accountability and visibility of contractors deployed in support of DoD, DOS and USAID.

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.

SPOT-ES does not collect information directly from the individuals, 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.