



PRIVACY IMPACT ASSESSMENT (PIA)

For the

SPOT & JAMMS (Synchronized Predeployment and Operational Tracker and Joint Asset Movement Management System)
--

Deputy Under Secretary of Defense for Business Transformation

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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 SPOT = 6501, JAMMS = 11857
- 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

SPOT: 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

A0715-9 DCS, G-4 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.

[Empty box for date of submission]

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

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. §§ 3013; National Defense Appropriations Acts (NDAA) 2008, Section 861; Homeland Security Presidential Directive/HSPD-12; Secretary of Defense; DoD Instruction 3020.41, Contractor Personnel Authorized to Accompany the U.S. Armed Forces; 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; 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 Instruction 8910.01, Information Collection and Reporting; DOD Directive 5015.2, DoD Records Management Program; Army Regulation 715-9, Contractors Accompanying the Force and E.O. 9397.

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) has been designated by the DoD as the central repository for information on contractors deploying with the force (CDF). Recently adopted by the Business Transformation Agency (BTA) as a Joint Enterprise system, it's the only system that supports the DoDI 3020.41 requirements to relate contract level information with individual contingency contractor employee information, including but not limited to contract and personal identity information (PII), contractor location and next of kin info. It also will support initial DoDI 3020.50 requirements on implementing weapons accountability procedures for Private Security Contractors by the end of December 2009. System records are populated by Company personnel via secure, Internet access and updated with current locations as individuals move throughout the area of responsibility (AOR). Location transactions for personnel and equipment are recorded by scanning at the point of service using the Joint Asset Movement Management System (JAMMS). Transactions are uploaded to the SPOT database and appended to the appropriate contractor deployee's record. SPOT is using evolutionary acquisition to incrementally deliver improved capabilities to a broad range of customers, spanning two Acquisition Phases, "Production & Deployment" and "Operations & Support." SPOT is hosted at the Acquisition, Logistics and Technology Enterprise Systems and Services (ALTESS) facility in Radford, VA and currently uses a tape backup system. Connections exist with Defense Manpower Data Center (DMDC), Army Knowledge Online (AKO), Federal Procurement Data System-Next Generation (FPDS-NG), Joint Contingency Contracting System (JCC-S), Global Exchange / Standard Procurement System (GEX/SPS), Deployed Theater Accountability System (DTAS), Biometrics Identification System for Access (BISA), and Defense Biometrics Identification system (DBIDS).

• The Joint Asset Movement Management System (JAMMS) is an information technology application developed to capture movement and location information about operating forces, government civil servants, and government contractors in specified operational theaters. JAMMS is being expanded to collect information on contractor acquired property in FY10. Each JAMMS unit consists of a laptop computer with one or two barcode scanners. JAMMS is a standalone system that has no external network connectivity. JAMMS workstations are set up at high traffic area data collection points to include dining facilities (DFACs), aerial ports of debarkation (APODs), central issue facilities (CIF), medical facilities, convoy staging areas, and Department of State (DOS) locations. Personal Identity Verification (PIV) compliant identity credentials (e.g., common access cards (CAC), defense biometrics identity system (DBIDS) credentials, letters of authorization (LOA), passports) are scanned for all personnel (e.g., armed forces, government civil servants, and contractors) going through a check point with a JAMMS scanner. JAMMS collects the document type and the document identifier for each credential that is scanned. JAMMS also collects the name, rank/pay grade and personnel category, e.g., contractor, military, civilian of each individual scanned. Persons boarding planes may be asked to provide their weight to ensure safety limits are not exceeded. JAMMS v. 3.0 retains this information on the laptop in an encrypted format for a limited period of time, routinely 30 days. This encrypted information is dropped to a CD/DVD and uploaded daily to SPOT where the document identifier is translated into a specific person. The location information is then appended to the existing SPOT record. If a matching record does not exist in SPOT, a mini-record with just the basic personal information and specific location is created in the SPOT database.

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

• Privacy risks were addressed as part of the SPOT and SPOT database development in accordance with DoD Information Assurance Certification and Accreditation Procedures (DIACAP). 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. For example, an authorized SPOT user who is an administrative person in Company "X" would only have access to Company "X" files

to enter and update information regarding their contract, their employees and deployment details to include PII data. Contracting officers would only have access to contracts managed by their Contracting Office to view and approve Letters of Authorization (LOAs) and enter government furnished services in accordance with the specified contract.

- Every SPOT user is verified by a member of the SPOT Enterprise Customer Support Team, who identifies and contacts the sponsor of the person to verify their need for access and what role the user should have within the SPOT system. A Combatant Commander and his authorized staff members would have access to information on the persons in their AOR just as a contractor company would have access to information on their employees.
- The risk of the total information contained in SPOT being compromised is very low as it is mitigated by limiting each user to the information they may access based on their role and their organizational affiliation as described above. Risk of any compromised PII would be to know the name, address, DOB and company that a person works for in support of U.S. interests. Records are kept for each user session and any unauthorized access requests are denied by the Customer Support Team and the software safeguards. While the person's social security number is collected, the risk of that being compromised is mitigated by limiting its display to the last four digits. This also means that the risk of identity theft is low as the data stored does not contain complete SSNs. The likelihood for misuse or enemy access to SPOT information is very low due to the sponsored user registration process and the likelihood that they would target individuals based on information obtained from SPOT is very low. Cyber threats are reduced by running the system on a DoD certified enclave and mitigation is in place using software intrusion detection. Additionally, the customer support desk is trained and has proven effective in countering social engineering attacks. There are three items of medical information collected: blood type, whether DNA is on file and whether a dental pantograph is on file. No risk to the individual has been identified if this information is compromised. Personal financial information is not collected in SPOT, so there is no risk of compromising that type of information, reducing the risk of financial fraud. The risk of losing a SPOT-generated LOA is similar to that of losing Defense Travel System (DTS)-generated Form 1610, Request and Authorization for TDY Travel of DoD Personnel. SPOT mitigates the risk of PII exposure by portraying only the last 4 numbers of the SSN. SPOT has a current 3-year Authorization to Operate (ATO), dated 4 Dec 08.
- Privacy risks were addressed as part of the JAMMS application development in accordance with DoD Information Assurance Certification and Accreditation Procedures (DIACAP). JAMMS privacy information is encrypted. JAMMS contains limited PII: name, personnel type, rank and weight. The risk of compromise is mitigated by having the data at rest encrypted as described above. The systems are physically locked in place. If compromised, there is virtually no risk that the information could be used as the perpetrator would require the code to crack the encryption. In the unlikely event JAMMS information was obtained, there is nothing available beyond knowing a named person was in a particular location at a particular time. The risk of any action against the individual is low as a name in and of itself is not enough to determine the specific person or their current location nor enough to allow for identity theft. The contractors who operate the JAMMS workstations do not have the ability to translate the encrypted information stored in JAMMS into personal information. JAMMS has a current one year ATO, dated 20 Nov 09.
- Risk is mitigated in SPOT and JAMMS 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.

Information is provided to individuals based on their association with a specific component entity. SPOT contains role-based security; therefore each user is provided access based on their specific role within their DoD component organization. Personnel are scanned by JAMMS regardless of their individual component assignment. JAMMS stations are operated by contractor personnel who do not have the ability to translate the encrypted personal information stored in the system.

Other DoD Components.

Specify.

In accordance with the 28 Jan 08 Defense Procurement and Acquisition Policy (DPAP) Memo, all contractors employed on DoD-funded contracts being performed in support of contingency operations anywhere in the world are to be entered in SPOT. Therefore, all DoD components require access to SPOT. Information is provided to individuals based on their association with a specific DoD entity. SPOT contains role-based security; therefore each user is only provided access based on their specific role within DoD. JAMMS stations are operated by contractor personnel who do not have the ability to translate the encrypted information stored in JAMMS into personally identifiable information (PII).

Other Federal Agencies.

Specify.

SPOT is Congressionally mandated for use by the Department of State (DoS) and the US Agency for International Development (USAID). The SPOT Team is having ongoing discussions with other federal departments for possible future use. The information is provided to individuals based on their association with a specific government entity. SPOT contains role-based security; and each user is provided access based on their specific role within the organization. Information is also provided to the General Accountability Office and members of Congress upon their request. JAMMS is being used at DoS as well as DoD locations. JAMMS stations are operated by contractor personnel who do not have the ability to translate the encrypted information stored in JAMMS into PII.

State and Local Agencies.

Specify.

Currently, SPOT is not used by State or Local Agencies. However, SPOT is mandated for DoD in any peacekeeping, humanitarian or military contingency operation. Therefore, JAMMS and SPOT will be used to support DoD contingency operations within the United States boundaries. When this occurs, all personnel entering the perimeter will be scanned by JAMMS to include state and local representatives such as government, medical, police and non-government organizations, e.g., Red Cross, that are among first responders to an emergency situation. There is no current guidance on use of SPOT and JAMMS for these persons. However, the Statement of Records Notice (SORN) does identify military and civilian employees, dependents, contractors and non-governmental organization personnel, volunteers, partner agencies personnel and members of the public who are supporting planned, ongoing, and historical contingency operations as potential categories of individuals covered by SPOT.

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

Specify.

Contractor personnel authorized to accompany the U.S. Armed Forces are covered by DFARS clause 252.225-7040 which requires use of SPOT and compliance with United States regulations, directives, instructions, policies, and procedures. Information is provided to individuals based on their association with a specific contractor company. SPOT contains role-based security; therefore each user is provided access based on their specific role within the company. When an employee transfers from one company to another, the losing company users are no longer able to view the individual's record. A small number of members of the SPOT Enterprise Customer Support Team have limited access to masked PII in order perform troubleshooting analysis for SPOT users. JAMMS stations are operated by contractor

personnel who do not have the ability to translate the encrypted information stored in JAMMS into personal information.

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

Specify.

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.

SPOT collection of privacy act information was initially announced in the Federal Register in September 2005. Persons were allowed to comment at that time and no comments were received. 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.

Individuals complete forms regarding PII as a part of the hiring process. Individuals have the opportunity to give their consent to the specific uses of their PII by signing these employment agreement and contractor human resources forms. Individuals can withhold their consent to the specific uses of their PII by not signing these documents.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Per DoD Federal Acquisition Regulation Supplement (DFARS) 252.225-7040, the companies using the SPOT/JAMMS systems application are required to comply with all applicable United State laws and regulations. To comply with the 1974 Privacy Act (PL 93-579) requires that individuals from which data is collected be provided with the rationale for the collection of the data, i.e., a Privacy Act Statement.

The Privacy Act Statement identifies the authority which allows the solicitation of the information; describes the principal purpose for which the information is intended to be used; lists the routine uses which may be made of the information gathered; explains whether disclosure of such information is mandatory or voluntary, and the effects, if any, of not providing the requested information.

Additionally, a record of some of the PII that has been collected is provided to the individual prior to deployment in the form of a Letter of Authorization (LOA), which identifies the person, their company / contract, and associates them to a specific mission in a defined country or countries within the AOR. A hard copy of their own LOA is provided to each deployee to carry on their person throughout their processing and deployment.

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.