DOD Privacy Impact Assessment (PIA)
for
Synchronized Predeployment and Operational Tracker (SPOT)

(Use N/A where appropriate)

1. Department of Defense (DoD) Component. **Deputy Under Secretary Defense for Business Transformation**

2. Name of Information Technology (IT) System. **Synchronized Predeployment and Operational Tracker (SPOT)**

3. Budget System Identification Number (SNAP-IT Initiative Number). **#1929**

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)). **#6501**

5. IT Investment (OMB Circular A-l 1) Unique Identifier (if applicable). **N/A**

6. Privacy Act System of Records Notice Identifier (if applicable). **A0715-9 DCS, G-4 DoD**

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date. **Pending**

8. Type of authority to collect information (statutory or otherwise). **DoD Instruction (DoDI) 3020.41, Defense Federal Acquisition Supplement (DFARS) Clause 252.225-7040 and associated Class Deviations, Congress, and the National Defense Appropriations Acts (NDAA) of 2005, 2006 and proposed NDAA language for 2008.**

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

   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, contractor location and next of kin info. The system is populated by Company personnel via secure, Internet access and updated with current locations as individuals move

throughout the area of operational responsibility (AOR). SPOT is in operations and support, is hosted at the Acquisition, Logistics and Technology Enterprise Systems and Services (ALTESS) facility in Radford, VA and currently uses a tape backup system. Fiscal Year 2007 funding was provided to establish a formal Continuity of Operations (COOP) site. Connections exist with Defense Manpower Data Center and Army Knowledge Online (AKO). Additional connections are planned with sister authoritative data systems.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.). **Information collected is presented in the attached Data Element Excel document.**
11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.). **Information is collected via secure entry (secure shell port 43) on the web and through automated connections. All Points, Protocols and Services (PPS) are on the approved PPS matrix, and are further enhanced by firewall rule sets on the Firewall located at Radford, VA. Security is mitigated to LOW.**
12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.) **The information collected is required to maintain accountability for contractors who accompany the U.S. armed forces and other persons who travel to support the U.S. Government.**
13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.). **The information is used to generate documents to approve travel for these persons, to contact contract and contractor company personnel regarding deployees, and to record their location when staying or traveling in operational environments to support U.S. missions.**
14. Describe whether the system derives or creates new data about individuals through aggregation. **The system aggregates counts of persons according to related data items, e.g., contract, company, sponsoring Government organization.**
15. Describe with whom the information in identifiable form will be shared, both within

the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.). **The information is provided to individuals based on their association with a specific contractor company or government entity. SPOT contains role-based security; therefore each user is only provided access based on their specific role and company / organization. For example, an authorized SPOT user who is an administrative person in Company "X" would have access to Company "X" files. Each of these SPOT users is verified by a member of the SPOT Customer Support Team, who identifies and contacts the sponsor of the person to verify their need for access and what roles that 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. As the central repository of contractor information, SPOT is engaged in discussions with the Department of State and other Federal Agencies. Just as described above, their access would be limited to the persons who are deployed in support of their organization's missions.**

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent. **Strategically, SPOT collection of privacy act information was 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. Routinely, company administrators enter the data. Individually, contractor company employees are able to become registered users of SPOT so that they can verify, maintain and update their personal profile information to ensure the accuracy of the data.**

Users who have been vetted for access to the individual tracker's company or organization as described in answer 15 will have access to these records also; and they are the ones whose role allows creation of deployment information.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form. **As stated in answer 16, individuals may be able to view their own records and make corrections to the personal information recorded therein. However, individual contractor deployees will not be able to modify contract or deployment information. Only those who are properly registered, vetted, and provided mission-specific access will be able to enter this type of information. Privacy Act information is collected and provided to the individual prior to deployment in the form of a letter of authorization (LOA), which identifies the person and associates them to a specific mission in a defined country or countries within the AOR. This LOA is viewable to those with access to the specific record and a hard copy is provided to the deployee to carry on their person throughout their processing and deployment. Vetting occurs as described in answers 15 & 16. User accounts are deactivated when SPOT is notified that they are no longer required. In theater, SPOT is used and updated by military/civilian personnel as a tracking tool on all deployed contractors in the AOR.**

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form. **Information is stored on a DoD approved and accredited infrastructure behind the AKO firewall, with access limited to those with proper credentials. SPOT recognizes three different credentials: AKO log in and password, Common Access Card (CAC) certificate, and DoD-approved software certificates (soft certs). Vetted users must have one of these identity credentials. Each user is registered for a specific role and permitted to create, read, update**

and delete only those items under their area of responsibility.

19. Identify whether the IT system or collection of information will require a System of Records Notice (SORN) as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur. **The SORN was published in the Federal Register: September 28, 2005 (Volume 70, Number 187, Page 56646-56647.**
20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures. **Privacy risks were addressed as part of the standard application and database development. As described in answer 18 above, information is stored on a DoD-accredited infrastructure, therefore risk is minimal. Xacta Corporation performed the accreditation. BTA issued an Interim Authority to Operate (IATO) on 8 June 2007. There is no risk involved in letting persons have the opportunity to review their data, as described in the answer to # 16 above, that option is available to persons whose data is collected. If a person objects to providing their data, then the contractor company has the right to refuse them employment. Notifications are not sent. No further risks have been identified.**
21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form. **Information is For Official Use Only in the Sensitive, but Unclassified category. Therefore, PIA should not be published.**

Preparing Official Theresa R. Miller (signature) 9/23/08 (date)
Name: Theresa R. Miller
Title: EPMO SPOT
Organization: PMO SPOT
Work Phone Number: 732-427-4670
Email: theresa.miller@us.army.mil

Information Assurance Official [signature] (signature) 9/23/08 (date)
Name: Bernard J. McGuinness (contractor)
Title: IAO SPOT
Organization: EPMO SPOT
Work Phone Number: 732-383-1125
Email: bernard.mcguinness@us.army.mil

Privacy Officer Chris M Forshey (signature) 4/21/2009 (date)
Name: Chris Forshey
Title: Privacy Officer, CIV BTA
Organization Chief of Staff/Chief, Privacy
Work Phone Number: 703.607.3952
Email: Chris.Forshey@BTA.mil

Reviewing Official [signature] (signature) (date)
Name: Michael Robinson
Deputy, Chief Information Officer
Organization: Chief of Staff/Chief, IT Services
Work Phone Number: 703.607.5146
Email: Michael.Robinson@BTA.mil