



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

PM Soldier Equipment - Standard Management Asset Readiness Tool (PMSEQ-SMART)

ASA(ALT) - PEO Soldier

### **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
- 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

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

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**

**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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1322.25, Voluntary Education Programs; DoD Instruction 1336.01, Certificate of Release or Discharge from Active Duty (DD Form 214/215 Series); Army Regulation 735-5, Policies and Procedures for Property Accountability; 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.

Web-based COTS application for managing inventory. SMART facilitates inventory management of Project Manager Soldier Protection & Individual Equipment (PM SPIE) managed items. Helps PM SPIE provide the Army the most advanced equipment in the most efficient manner. The System provides planning, execution and data Archive capability for all Fielding events supported by the PM. Provides an E-Order capability for the CIFs.

PM SPIE uses a portable fielding system called the Standard Management Access Readiness Tool (PMSEQ-SMART) System. SMART allows users to access the required report areas via the DoD Non-classified Internet Protocol Router Network (NIPRNet) or Internet. The data is uploaded, on a daily basis, into the SMART System to support PM SPIE Planning, Reporting, Discrepancy resolution, and Archive requirements. The data is re-encrypted once in the SMART System.

The type of PII collected is personal information.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (fire, flood, etc.). The potential risk in regard to collection/transfer/storage of the data would specifically be related to the encryption and management of the data. The users will use Encrypted File System (EFS) as part of the mitigation in the encryption of the data, as documented in the SOP for the Fielding System Technicians using Army approved encryption software. The encrypted data transfer from PM SPIE fielding sites / events requires the transfer via Secure File Transfer Protocol (SFTP) to the PM SPIE SFTP Server, maintained in the NEC Server Room. After QA analysis, the data is uploaded into the SMART System Archives. The handling of the PII Data is strictly managed and controlled to mitigate the risk of loss, theft or misuse from the collection, through transfer and archiving into the SMART System.

**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.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

**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.

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

The collection of the data is required for in-processing Soldiers at PM SPIE fielding sites / events and is later needed to post the fielding data to clothing record change documents in the Army Installation Support Module-Central Issue Facility (ISM-CIF) System as well as the SMART System Archives. The SORN and AR 710-2 require that Soldier clothing records be distinguished by the SSN.

**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.

The data collected during in processing establishes the local Hand Receipt record for each soldier at that fielding site / event. At the conclusion of the fielding event, the data is transferred to Soldier clothing records maintained in the ISM-CIF System, the requiring system of record. The data is also posted to the SMART System Archives. The SSN is used to place the data into the correct clothing record and is Army mandated.

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

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

Describe each applicable format.

PRIVACY ACT STATEMENT

Authority: 10 U.S.C. 3013, Secretary of the Army and DoD Directive 3020.26, The Defense Continuity Program.

Purpose: To document names and phone numbers of persons to be notified in emergency situations.

Routine Use: None. The 'Blanket Routine Uses' apply.

Disclosure: Voluntary. Failure to supply this information may result in not being notified of a potential emergency to include acts of nature, accidents and technological and/or attack-related emergencies.

**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.