PRIVACY IMPACT ASSESSMENT (PIA)

For the

Property Book Unit Supply Enhanced (PBUSE)
HQDA G4 - Army Material Command (AMC) - Communications-Electronics Command (CECOM)

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: 260 (DA05667)
- ☐ **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 S800.20 Military Clothing Database (October 26, 2012, 77 FR 65

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.

S800.20 Military Clothing Database (October 26, 2012, 77 FR 65370)
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 1338.5, Armed Forces Clothing Monetary Allowance Policy; 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.

Property Book Unit Supply Enhanced (PBUSE) began in May 2000 as a Web-based pilot custom software development effort that would replace both the Standard Property Book System-Redesign (SPBS-R) and the Unit Level Logistics System S-4 (ULLS-S4) systems. A successful property book Software Acceptance Test (SAT) was conducted from February through March 2002 at Fort Hood, Texas, and the migration of SPBS-R to PBUSE began in June 2002. The Unit Level SAT was conducted in USARPAC, Fort Hood, San Antonio, Texas (USARC), and Little Rock, Arkansas (Army National Guard) during October through November 2002.

The purpose of PBUSE is the Army's Web-based, fully interactive, combat support property accountability system. PBUSE is a modernized supply and property module that integrates supply operations and property accountability in all Army units. The centralized PBUSE Web and database servers are located at the Software Engineering Center Lee, Tactical Logistics Directorate, Fort Lee, Virginia. The servers operate behind a reverse proxy firewall employing load balancers that prevent direct access to the servers by the users. The load balancers control the user traffic to the Web servers through reverse proxy and firewall rules that preclude direct access to the servers. User login is via Common Access Card (CAC) with Army Knowledge On-Line (AKO) accounts. The user computer is a commercial personal laptop that operates in peacetime and wartime.

PBUSE is an unclassified system which uses permission control to manage access to data. The system is accessed through CAC only authentication. The system is employed by the Active Army, Army Reserve and Army National Guard and provides both sustaining base and tactical functionality. In the sustaining base, PBUSE operates over NIPERNet/Internet connections. In the tactical environment, PBUSE uses the Very Small Aperture Terminal (VSAT) or Combat Support Automated Information Systems Interface (CAISI). The Army Audit Agency (AAA) certified that PBUSE was Federal Financial Management Improvement Act (FFMIA) Chief Financial Officer (CFO) compliant for Modified Tables of Organization and Equipment (MTOE) in July 2002; in September 2004, AAA certified the software as also being compliant for Tables of Distribution Allowance (TDA). PBUSE provides real time property accountability, Logistics The Army Authorization Documents System (LOGTAADS) updates, Serial Number Tracking, asset adjustments, lateral transfers, authorization updates, and manages basic and operational loads and hand receipts.

The type of PII collected is personal, military, and work-related information.

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

Risk to the individual includes potential compromise of personal financial data if Personally Identifiable Information (PII) is disclosed.

All personnel accessing government computer information are required to undergo and receive at the minimum a favorable National Agency Check. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment. The System Administrator defines specific access requirements dependent on each user's role. Each specific application in the system may further restrict access via application-unique permission controls. There is weekly monitoring of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). Files transferred across the Internet/NIPRNet are encrypted using Virtual Private Network (VPN) or Advanced Encryption Standard (AES) 256-bit encryption. Full Social Security Numbers (SSN)'s are displayed only to a limited number of authorized users. Other authorized users can see the last 4 digits. SSN data is encrypted within the database and the database back-ups.

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 will be made available to Army installation Central Issue Facility (CIF) for the purpose of tracking Organizational Clothing and Individual Equipment (OCIE).

☒ **Other DoD Components.**

Specify. Information will be shared with Defense Finance and Accounting Service (DFAS)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Station-specific staff to CIF may be contracted personnel. These personnel are required to receive a favorable National Agency Check.

☐ **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.

Individual can refuse to provide PII. As a consequence, the individual will not be issued OCIE.

(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.

The individual may choose to not provide PII and refuse OCIE.

(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.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

Privacy Advisory Statement is attached. The DLA rules for accessing records or contesting contents and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Privacy Act Office, Headquarters, Defense Logistics Agency, ATTN: DGA, 8725 John Kingman Road, Stop 2533, Fort Belvoir, VA 22060-6221