PRIVACY IMPACT ASSESSMENT (PIA)

For the

Deployed Theater Accountability System (DTAS) NIPR
Program Executive Office Enterprise Information Systems - Army Human Resource System (PEO EIS - AHRS)

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: 13222 (DA200662)
- ☐ **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 A0715-9a G-1 (PENDING publishing at the Federal Register)

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 Submitted request 15 March 2013

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, Secretary of the Army; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1074, Medical Care and Tracking and Health Surveillance in the Theater of Operation; 10 U.S.C. 991, Management of deployments of members and measurement and data collection of unit operating and personnel tempo; 10 U.S.C. 482, Quarterly reports: personnel and unit readiness; 10 U.S.C. 165, Combatant commands: administration and support; 10 U.S.C. 166, Combatant commands: budget proposals; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters; DoD Directive 1400.31, DoD Civilian Work Force Contingency and Emergency Planning and Execution; DoD Instruction 1400.32, DoD Civilian Work Force Contingency and Emergency Planning Guidelines and Procedures; DoD Directive 1404.10, DoD Civilian Expeditionary Workforce; DoD Instruction 3020.41, Contractor Personnel Authorized to Accompany the U.S. Armed Forces; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); 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; DoD Instruction 8910.01, Information Collection and Reporting; Chairman of the Joint Chiefs of Staff Manual 3150.13C, Joint Reporting Structure - Personnel Manual; Army Regulation 715–9, Operational Contract Support Planning and Management; 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.

The Deployed Theater Accountability System (DTAS) is the Army's personnel tracking system. DTAS provides near real time data on individual personnel status, grid location (or city/state), unit strengths, and deployment history.

The information collected is required for establishing and maintaining central personnel records repository for personnel accountability, strength management reporting, and compliance with deployment health policies and readiness reporting.

The DTAS is a web enabled software package that resides on the military SIPRNet or NIPRNet and contains accountability data for military, civilian, and contractor personnel in a deployed theater by unit, day, and location. Overall, DTAS consists of an Enterprise Server Suite, Theater Server Suite(s), and the unit Mobile System(s).

DTAS is both a client and server application to allow tactical units uninterrupted access to their data while still updating higher HQ when communications are available, and a Web-Enabled application for Theater/ Command level personnel to manage units and analyze the data. DTAS can provide commanders and personnel specialists with real-time accountability of deployed military personnel, civilians, and contractors' in-Theater.

The DTAS Mobile User System hierarchy extends theater level command down to tactical battalions and separate companies, using each unit's existing computer infrastructure linked into the theater's network. Each Mobile system reports on one or more units personnel, and synchronizes with the Theater Server Suite. The Theater Suite provides deployment history data to the Enterprise Suite. The Enterprise Suite interfaces with numerous personnel management systems to provide DTAS with descriptive personnel data, eliminating the need for duplicative data entry.

The PII collected is military, medical, personal, and employment.

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

DTAS NIPR operates on the NIPRNET and users must be granted a unique DTAS username and password, the risk of losing PII security is very low. To mitigate this risk, usernames are audited quite frequently to ensure users genuinely have a need to know.

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. Program Executive Office Enterprise Information Systems (PEO EIS)
Product Director Army Human Resource System (PD AHRS)
Army Human Resources Command (HRC)
Coalition Forces Land Component Command (CFLCC) G1,

Inspector General (IG)
Department of the Army (DA)

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC)

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. Hewlett Packard (HP) in compliance with AR 25-2 Information Assurance.

Language from Contract: "The Government shall define and maintain security requirements for protecting the system and data. The DTAS NIPR application must have the capability to maintain SECRET data. For all other AHRS applications both the data and systems are sensitive but unclassified. The data must also comply with the U.S. Government Privacy Act Requirements."

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

Specify. N/A

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.

Privacy Act Statement - Form is provided to personnel at the CONUS Replacement Centers (CRCs) during the pre-deployment certification process prior to deployment.

(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.

Sign or revoke their Privacy Act Statement

(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 Act Statement.

Army Regulation 340-21 details individuals rights to access PII and rules for disclosure to third parties.

Whenever personal information is requested from an individual that will become part of a system of records retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act Statement.

All forms and databases used to populate DTAS have a Privacy Act Statement and Advisory on them. At initial sign on, a Privacy Act Statement appears on the DTAS screens."

Language from Privacy Act Statement/Advisory.

" You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.