PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

TAPDB-AE - TOTAL ARMY PERSONNEL DATA BASE - ACTIVE ENLISTED

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

08/25/20

US Army Deputy Chief of Staff for Personnel / Human Resources Command (HRC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Total Army Personnel Data Base - Active Enlisted is the central database for all information pertaining to Active Army Enlisted Soldiers. It contains a set of logically integrated and physically distributed databases.

Types of PII collected include personal, contact, dependent, emergency contact, medical, disability, employment, education, and military record data.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Identification and data matching: TAPDB-AE is the enterprise database for the Active Army Enlisted personnel processing systems. Soldier information is collected and provided to associated IT systems for the purpose of manning the force, projecting unit strength, assignments, reassignments, promotions, demotions, personnel accountability, regimental affiliations, education information (both military and civilian), awards, and deployment history. Both mission-related and administrative use: TAPDB-AE data are used for a wide variety of personnel management purposes, to include providing data to other Army systems such as the Integrated Total Army Personnel Data Base, and to assist in validation of data within other Army systems.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII is collected only through electronic extraction via a secure network connection from other systems. Since data are not collected directly from individuals they are not provided either a Privacy Act Statement or a Privacy Advisory from TAPDB-AE. However, individuals are afforded an opportunity to object and implicitly consent to capture and use of their information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

PII is collected only through electronic extraction via a secure network connection from other systems. Since data are not collected directly from individuals they are not provided either a Privacy Act Statement or a Privacy Advisory from TAPDB-AE. However, individuals are afforded an opportunity to object and implicitly consent to capture and use of their information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

Since PII is not collected directly from individuals they are not provided a Privacy Act Statement or Privacy Advisory when the data are collected by TAPDB-AE. However, individuals are provided a Privacy Advisory at the time of employment or enlistment in the Department of the Army, implicitly consenting to use of their data for personnel management purposes.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Staff principals in the chain of command, Department of the Army Inspector General, Army Audit Agency, US Army Criminal Investigation Command, US Army Intelligence and Security Command, Provost Marshall General, and the Assistant Secretary of the Army for Financial Management and Comptroller.
☒ Other DoD Components	Specify.	Office of the Under Secretary of Defense for Personnel and Readiness, Personnel Readiness Information Management; Defense Finance and Accounting Service; Defense Intelligence Agency; US Air Force; US Marine Corps; US Navy; Joint Services Records Research Center; Department of Defense Inspector General, Defense Manpower Data Center, and Defense Criminal Investigative Service.
☒ Other Federal Agencies	Specify.	National Archives and Records Administration; Department of Veterans Affairs; Office of Personnel Management; Department of Homeland Security; Federal Bureau of Investigation; State Department; Treasury Department; Department of Labor; Department of Justice; National Reconnaissance Office; Social Security Administration; and Office of the President of the US.
☒ State and Local Agencies	Specify.	State and local law enforcement agencies.
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Science Applications International Corporation contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentiality and security of an individual's PII. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of a work day. Contractual language directs and requires each SAIC employee in support of the database to have a valid Secret clearance prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U.S. Code Section 552a, and all applicable agency rules and regulations.
☐ Other *(e.g., commercial providers, colleges)*.	Specify.	N/A

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

PII is collected electronically via secure connections from the following existing DoD information systems: Assignment Satisfaction Key, Enterprise Service Bus, Enlisted Distribution and Assignment System, Army Knowledge Online, and Army Training Requirements and Resource System.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [x] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

N/A

k. 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 must be consistent.

- [ ] Yes
- [x] No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date N/A

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

Per APO... Not considered a system of record. Middleware IT system processing source data for multiple Systems of Records that are covered by A0600-8-104 AHRC, Army Personnel System. System to be subsumed by IPPS-A (INC II R3) 20180205 (CMB)

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-AU-06-0008

(2) If pending, provide the date the SF-115 was submitted to NARA. N/A

(3) Retention Instructions.

KE6. Event is when database is discontinued. Keep until event occurs then delete data 6 years after ITAPDB is discontinued.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 United States Code (USC) Section 301, Departmental Regulations; 10 USC Section 3013, Secretary of the Army; Army Regulation (AR) 600-8-6, Personnel Accounting and Strength Reporting; AR 600-8-104, Military Personnel Information Management/Records; and Executive Order 9397 as amended (SSN).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

If 'No' enter: "System does not collect PII from 10 or more members of the general public in a one-year period."