PRIVACY IMPACT ASSESSMENT (PIA)

For the

Soldier Management System (SMS) on USAACE VWE

U.S. Army Training and Doctrine Command (TRADOC)

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: 16776/ AITR - DA303989 - USAACE VWE
- ☐ **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: A0350-20a TRADOC

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.

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 3583 Requirement of Exemplary Conduct; DoD Directive 6490.2E, Comprehensive Health Surveillance; DoD Instruction 6490.03, Deployment Health; Army Regulation 40-5, Preventative Medicine; Army Regulation 40-66, Medical Record Administration and Health Care Documentation; Army Regulation 350-1, Army Training and Leader Development; Army Regulation 350-10, Management of Army Individual Training Requirements and Resources; Army Regulation 600-8-104, Military Personnel Information Management/Records; Army Regulation 600-20, Army Command 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.

The purpose of the system is the consolidation of personnel information from pre-existing databases for local use by U.S. Army Aviation Center of Excellence G1/G4 to track and maintain personnel actions for assigned members. The databases that act as a source for SMS data are the Total Officer Personnel Management System (TOPMIS) and the Electronic Military Processing Office (eMILPO). The types of personal information collected could include names, addresses, social security numbers, and/or birthdates.

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

The privacy risks are minimal in that the data is safeguarded by CAC authentication, specific permissions on a per-item basis, and accessibility only from within a .MIL network. Access to personal information is restricted to those who require the records in the performance of their official duties. The database is secured via Transparent Data Encryption which encrypts the database file on the server using AES256.

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. U.S. Army Aviation Branch, Department of the Army Inspector General, Army Audit Agency, U.S. Army Criminal Investigation Command, United States Army Intelligence & Security Command (INSCOM), Provost Marshall General, National Guard Bureau (NGB), and Army Reserve.

☒ **Other DoD Components.**

Specify. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General and Defense Criminal Investigation Service.

☐ **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.

The individual implicitly consents to the capture and use of PII at the time of employment, commissioning, or enlistment in the Department of Defense, at which time, they are provided a privacy advisory. Forms containing SSNs must meet the DOD Acceptable Uses in reference to the SSN Reduction Plan in order to require the SSN. Privacy considerations are taken into account during the original collection of PII as form fields. Privacy considerations are taken into account during the original collection of PII in TOPMIS and eMILPO. These previously and separately collected data are populated prior to input into the SMS.

(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 implicitly consents to the capture and use of PII at the time of employment, commissioning, or enlistment in the Department of Defense, at which time, they are provided a privacy advisory. Forms containing SSNs must meet the DOD Acceptable Uses in reference to the SSN Reduction Plan in order to require the SSN.

(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.

☐	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☒	**None**

Describe each applicable format.	PII data is not directly collected from individuals, and is originally collected in Total Officer Personnel Management System (TOPMIS) and the Electronic Military Processing Office (eMILPO) prior to porting into SMS.

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.