PRIVACY IMPACT ASSESSMENT (PIA)

For the

Senior Enterprise Talent Management System
Army

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: 12077 (DA 194163)
- ☐ **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: A0690-200 DAPE

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; Army Regulation 690-200, General Personnel Provisions

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.

SETM (formerly named CTMS) provides for the Secretary of the Army's Senior Civilian Education and Development Program by restructuring/reordering the Profile, Assessment, Board, Talent Management and Administrator screens and capabilities to emulate and better link to those in use for Senior Executives. The master profile provides useful information regarding the employee including personal information, current assignment information, goals and accomplishments, career chronology, prior year performance ratings, significant awards and accomplishments, education, training, licenses and certifications, language skills, publications, professional memberships and associations, professional Boards, current year assessment results, individual competencies, and future executive position preferences.

The types of PII collected pertain to personal, employment, and educational information.

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

This system is CAC access only. Limiting access to CAC users only helps safeguard privacy. Army Analytics Group (AAG) implements the following to protect PII:

1) Removal of Full SSN (only last 4 is retained) and replaced with internal sequence number. The cross reference table is managed in a separate location from the database for the CSLDD application and is encrypted at rest.

2) Oracle Transparent Data Encryption is implemented for the CSLDD database to ensure data is encrypted at rest.

3) Access to any data is limited by security roles and applied so that only appropriate personnel can see PII for a particular person.

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus we believe the risk to the individual's privacy to be minimal.

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. Army Civilian and Military Employees in grades GS 14/15, SES, COL and General Officers, to include Army Civilian Human Resources Agencies and U. S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command, US Army Equal Employment Opportunity (EEO) Community, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller, The Executive Office of the HQDA, The Army Secretariat, The Army Staff, and all Army Components which include the Army Commands.

☐ **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.

The following contractors have access to the system: Booze Allen Hamilton; iBASEt. Each contract has language similar to the content below.

1.6.7 Security Requirements:

1.6.7.1 The contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information which may involve the contractor or the contractor's personnel or to which they may have access may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at government expense during the course of this contract are the property of the government. At the time that the solicitation is issued, it should be accompanied by a Contract Security Specification, DD Form 254, in accordance with DoD Directive 5220.22-M, Department of Defense Industrial Security Manual for Safeguarding Classified

Information, and any revisions, thereto, as well as Industrial Security Regulation DoD 5220.22-R. Failure to safeguard and classified/privileged information which may involve the contractor or/or the contractor's personnel or to which they may have access may subject the contractor and/or contractor's personnel to criminal liability under Title 18, section 793 and 7908 of the United States Code.

1.6.7.2 SecArmy memorandum dated 28 January 2006 on Contractor Verification System (CVS) Implementation provides guidance and instructions for the implementation of the CVS Army-wide. IAW that guidance, the authorizing official (Contracting Officer Representative (COR)), Contracting Officer Technical Representative (COTR), Contracting Officer, or other approving officials), the contractor's sponsor, approves issuance of the CAC through the automated CVS system. The COR in the BPA is the designated Trusted Agent (TA). Further delegation of that authority is determined at the installation level. The contractor's CVS applications under this task order should clearly cite the contract and task order numbers identified on the DD Form 1155 for this task order.

1.6.7.3 Physical Security. The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials

shall be secured.

☐ **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 information in this system is provided by the Defense Civilian Personnel Data System and is used for centralized management and professional development of senior Army Civilians. Individuals can object to the collection of their PII by not submitting applications to apply for the SETM programs.

(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 system is a volunteer system. Individuals must voluntarily submit applications for training in this system. Applicants must physically submit applications for information to be passed along to Commanders and HQDA staff.

Individuals can withhold consent by not submitting applications for training.

(2) If "No," state the reason why individuals cannot give or withhold their consent.