PRIVACY IMPACT ASSESSMENT (PIA)

For the

Student Management System - Command and General Staff College (SMS-CGSC)
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: 16400 / DA302877
- ☐ **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 and A0608b CFSC

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; 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; AR 608-1 Army, Community Service; DA PAM 600-8-101, Personnel Processing; AR 608-75, Exceptional Family Member; AR 165-1, Army Chaplain Corps Activities; and E.O. 9397 (SSN), as amended. Standardized Student Records System purpose is to obtain training, education, experiential learning, personal, and biographical data to present a comprehensive and personalized view of the student record, course enrollment, course completion, official grade transcript, statistical studies to improve training and testing methods, and course catalog information. Records are created to assist leadership to instill an ongoing attitude of comprehensive, continuous, and consistent military health surveillance to implement early intervention and control strategies to promote and safeguard the moral, the physical well-being, and the general welfare of personnel at TRADOC organizations.

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.

Standardized Student Records System purpose is to obtain training, education, experiential learning, personal, and biographical data to present a comprehensive and personalized view of the student record, course enrollment, course completion, official grade transcript, statistical studies to improve training and testing methods, and course catalog information. Records are created to assist leadership to instill an ongoing attitude of comprehensive, continuous, and consistent control strategies to promote and safeguard the moral, the physical well-being, and the general welfare of personnel. Types of personal information collected are name, Social Security Number (SSN), Date of Birth, Gender, Race/Ethnicity, Place of Birth, Personal Cell Telephone, Home Telephone Numbers, Mailing/Home Address, Security Clearance, Emergency Contact Information: Spouse Information, Marital Status, Child Information (name and age), Military Records, Emergency Contact and Education Information.

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

There is minimal risk associated with the PII collected, however, it is safeguarded. This system is hosted on an Army installation, in a secure environment. Building security is through police patrols, installation fences, key card access, building-server room alarms and cameras. System access is through the Army Network Enterprise Center's firewall. Each user requires a user ID and password (which has to be changed each 90 days). Direct access to the database is restricted to authorized System Administrators (SAs) only. Servers are located in a cipher locked room and access is controlled by the SA. Any person having access to personally identifiable information (PII) is specific only to them or have a need to know in order to perform official government duties. Data is restricted by roles and permissions. Access is granted once they have been authenticated in the pertinent system through an incorporated security process, Common Access Cards (CAC). All SA personnel with access to the database are trained in Security+ certifications, to ensure they are current on new security standards.

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 Human Resources Command

☒ **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. Contractor: General Dynamics Information Technology. Contract number W911S0-11-D-0010. Contractor personnel will comply with the following Operations and

Communications Security procedures under this Performance Work Statement (PWS): All draft deliverables under this PWS and working papers associated with them will be shredded prior to recycling or disposal. Drafts in electronic media will be deleted or erased IAW current Army BBP, prior to reusing the diskette or space on a PC hard drive or shared server space. Final versions of products under this PWS will be delivered to the government as specified elsewhere. Apply "For Official Use Only" (FOUO) cover sheets to all draft and final deliverables under this PWS. Contractor personnel may disclose to non-DOD personnel, other than contractor personnel executing this same PWS, only the general nature of their work under this PWS (i.e. "I work for ___ Corp providing automation support for Army training programs." Contractor personnel will not transmit any sensitive information over unclassified information networks. Contractor personnel may consult with the COR if they are uncertain whether particular information is sensitive. Government furnished telecommunication and electronic communication systems and equipment, specificially including electronic mail systems, are for official use only in furtherance of the PWS. Contractor personnel will limit inter net access to the minimum time necessary to accomplish the official inquiry or research in furtherance of the PWS. Contractor personnel will respect all electronic communication advisories, virus warnings, and use restrictions on government-furnished telecommunications and electronic communications systems and equipment and give access to government automation security and maintenance personnel upon request. Contractor personnel shall review the provisions of AR 25-2, Information Assurance, prior to using government-furnished telecommunications and electronic communications systems and equipment. The contractor shall provide evidence of this review to the COTR for each member of the contractor staff working on the PWS. CAC Fort Leavenworth currently has an Acceptable Use Policy (AUP) that will require ALL contractor employees to review and sign acknowledging understanding and compliance of said policy. Any contractor employee violating the AUP may require immediate removal.

☐ **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.

(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.

(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.

Privacy and Security Notice
The Command and General Staff College Web Site is provided as a public service by the Command and General Staff College and the Directorate of Educational Technology.
In Accordance with Title 5, U.S.C. § 552a (Privacy Act of 1974) as implemented by the Federal Register, Department of Defense, Department of the Army, 32 CFR Part 505, The Army Privacy Program; Final Rule, protected personal information will not be disclosed from the Standardized Student Records System to any commercial enterprise or representative thereof or to any individual outside the Department of Defense. The Student Record Form will be safeguarded IAW paragraph § 505.2, of the Federal Register 61680. When updated, obsolete copies will be destroyed as required by paragraph 4-501, AR 25-55, The Department of the Army Freedom of information Act Program.
Information presented on the CGSC web site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.
For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
Except for authorized law enforcement investigations, no other attempt are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for