PRIVACY IMPACT ASSESSMENT (PIA)

For the

CCIMM - CADET COMMAND INFORMATION MANAGEMENT MODULE

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

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: 8247 DA121220
- ☐ **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 A0601-210 AHRC

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 United States Code (USC) 301, Departmental Regulations; 10 USC 503-504, Persons Not Qualified; 10 USC 2101-2111, Reserve Officer Training Corps; 10 USC 3013, Secretary of the Army; Army Regulation (AR) 145-1, Senior Reserve Officer Training Corps Program: Organization, Administration, and Training; AR 350-1, Army Training and Leader Development; AR 601-100, Appointment of Commissioned Officers and Warrant Officers in the Regular Army; AR 601-222, Armed Forces Military Personnel Accession Testing Programs; AR 614-100, Officer Assignment Policies, Details and Transfers; and Executive Order 9397 as amended (SSN).

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 Cadet Command Information Management Module (CCIMM) is the lifeline for the US Army Cadet Command (USACC) between strategic management and mission execution at battalion level. CCIMM provides an automated process to manage Reserve Officer Training Corps cadets from acceptance into the program to Army Leader. Cadets are retained, trained, paid, branched, and accessed in CCIMM. The system is USACC's baseline of information for strategic decisions, budgeting, recruiting, and marketing.

Types of PII collected include personal, contact, dependent, financial, medical, employment, education, and military personnel data.

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

The system and its components are maintained in a controlled, secure facility. Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Employees and appropriate contractor personnel are required to obtain security/information assurance training and certification based on system access levels and level of assigned responsibility. Data are passed via secure wide area networks or via use of virtual private networks. Due to the level of safeguarding, we believe the risk to individuals' 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. US Army Military Academy, Department of the Army Inspector General, Army Audit Agency, US Army Criminal Investigation Command, US Army Intelligence and Security Command, Army Provost Marshal General, US Army Cadet Command, US Army Recruiting Command, Army Deputy Chief of Staff (DCS) G-1, Army DCS G-2, Personnel Security Investigation Center of Excellence, US Army Reserve Command, and US Army Training and Doctrine Command.

☒ **Other DoD Components.**

Specify. Department of Defense Inspector General, Defense Criminal Investigative Service, Defense Finance and Accounting Service (DFAS), US Military Entrance Processing Command, National Guard Bureau, Defense Manpower Data Center, Defense Security Service, Office of the Under Secretary of Defense (OUSD) for Personnel and Readiness, and Office of the Under Secretary of Defense for Intelligence.

☒ **Other Federal Agencies.**

Specify. Office of Personnel Management, Selective Service System, Social Security Administration, Department of Justice (FBI).

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. Science Applications International Corporation (SAIC) contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentially 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 system 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. 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.

Contracted cadets are afforded the opportunity to object at the time their PII is collected, and are provided Privacy Act Statements when providing their data via DD Form 2005, DA Form 597, and/or DA Form 597-3.

(2) If "No," state the reason why individuals cannot object.

N/A

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.

Contracted cadets are given the opportunity to consent to the specific uses of their PII as documented via CC Form 137-R at the time that their PII is collected.

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

N/A

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.

DD Form 2005 contains the following:
1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SSN: Sections 133, 1071-87, 3012, 5031 and 8012, title 10 USC and Executive Order 9397.
2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED: This form provides you the advice required by The Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.
3. ROUTINE USES: The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to: Aid in preventive health and communicable disease control programs and report medical conditions required by law to federal, state and local agencies; compile statistical data; conduct research; teach; determine suitability of persons for service or assignments; adjudicate claims and determine benefits; other lawful purposes, including law enforcement and litigation; conduct authorized investigations; evaluate care rendered; determine professional certification and hospital accreditation; provide physical qualifications of patients to agencies of federal, state, or local government upon request in the pursuit of their official duties.
4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION: In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED. This all inclusive Privacy Act Statement will apply to all requests for personal information made by health care treatment personnel or for medical/dental treatment purposes and will become a permanent part of your health care record. Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

DA Forms 597 and 597-3 contain the following:
AUTHORITY: Title 10 USC, Sections 2101 through 2111, and 3013. Title 5 USC Section 301.
PRINCIPAL PURPOSE: To specify the contractual agreements and obligations and to document contracting in the Army Senior Reserve Officers' Training Corps Nonscholarship Program.
ROUTINE USES: This form will be maintained in the cadet's Military Personnel Records Jacket and becomes a permanent part of the official personnel records as confirmation of enrollment, contracting,