PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Accessions Command Integrated Automation Architecture (AAC-IAA)
Army Training and Doctrine Command, U.S. Army Accessions Command (USAAC)

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	76 (DA00489)
☐	**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 007-21-01-20-02-6040-00

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 TRADOC; A0601-210a USAREC; A0601-210b USARF

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 007-21-01-01-20-02-6040-00-404-142

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.

Comment: Only list the authority once, don't have to list the same authority each time. (Fixed)
10 U.S.C. 503 and 510
10 U.S.C. 1588, Authority to accept certain voluntary services
5 USC 3111, Acceptance of volunteer service
26 U.S.C. 6041, Information at Source
10 U.S.C. 2101-2111, Reserve Officer Training Corps, and 10 U.S.C. 3013, Secretary of the Army; Army Regulation 145-1, Senior Reserve Officer's Training Corps Program: Organization, Administration, and Training; Army Regulation 145-2, Junior Reserve Officer's Training Corps Program: Organization, Administration and Training, and E.O. 9397 (SSN)
10 U.S.C. 2031, Junior Reserve Officers' Training Corps
Army Regulation 350-1, Army Training and Leader Development
Army Regulation 601-100, Appointment of Commissioned and Warrant Officers in the Regular Army
10 U.S.C. 504, Persons not qualified; Army Regulation 601-210, Regular Army and Army Reserve Enlistment Program
Departmental Regulations; AR 601-210, Active and Reserve Components Enlisted Program
5 U.S.C 301; AR 614-100, Officer Assignment Policies, Details, and Transfers; AR 614-200, Enlisted Assignments and Utilization Management
10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 601-222, Armed Services Military Personnel Accession Testing Programs

10 U.S.C. 8013, Secretary of the Air Force, 10 U.S.C. 5013, Secretary of the Navy; DoD Directive 1145.2, United States Military Entrance Processing Command; Army Regulation 601-270/Air Force Regulation 33-7/Marine Corps Order P1100.75A, Military Entrance Processing Station (MEPS); MEPCOM Regulation 680-3, U.S. Military Processing Command Integrated Resources System (USMIRS)
Army Regulation 351-1, Individual Military Education and Training

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 US Army Accessions Command (USAAC) Integrated Automation Architecture (AAC-IAA) encompasses the entire automation support for an accessions and recruiting mission that operates primarily in the public space. The AAC-IAA is an Information Technology solution supporting Total Army (Active, Reserve, Army National Guard) Recruiting. The initial cornerstone of the AAC-IAA is a software component originally referred to as the Army Recruiting Information Support System (ARISS). It is now a sub-component within the larger, integrated architecture (AAC-IAA) which is in the maintenance and sustainment phase.

The purpose of this system is to assess, qualify and manage applicants for the purpose of accessing the most qualified into the Army. PII is used to verify medical, education, citizenship, law violations, and test score eligibility to process them to join the Army.

Information that is collected includes personal information, financial information, medical information, disability information, law enforcement information, employment information, military records, emergency contact, education information.

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

Due to the level of safeguards in the AAC-IAA, we believe the risk to individual's privacy to be low. Risk is mitigated by user passwords, firewalls, antivirus software, CAC access and data-at-rest protection software on portable laptops.

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. United States Army Military Academy, Army Surgeon General, Army Recruiting Command, Army National Guard, Army Accessions Command, Army Law Enforcement, Human Resources Command, DA G1, Army Staff Principals, Department of the Army Inspectors General, Army Audit Agency, Army Criminal Investigation Command, Army Intelligence and Security Command, Provost Marshal General, Assistant Secretary of the Army (Financial Management & Comptroller), and Assistant Secretary of the Army (Manpower & Reserve Affairs). Army Deputy Chief of Staff for Personnel, Army Medical Department, Army Research Institute, Army Reserve Command, Army Training and Doctrine Command, Army Knowledge Online,

Army Learning Management System, Army Office of Economic Manpower Analysis

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service, US Military Entrance Processing Command, Office of Economic and Manpower Analysis, Defense Manpower Data Center, Office of the DoD Inspector General, Defense Criminal Investigative Service, and Medical Facilities. Defense Security Service, National Guard Bureau, Office of the Secretary of Defense Personnel and Readiness, Office of the Secretary of Defense

☒ **Other Federal Agencies.**

Specify. Office of Personnel Management, Federal Aviation Administration, Department of Veterans Affairs, Selective Service System, Social Security Administration, Department of the Treasury, Department of Homeland Security, Department of Justice, Department of Health and Human Services, Federal Law Enforcement and Confinement/Correctional Agencies

☒ **State and Local Agencies.**

Specify. State and Local Law Enforcement Agencies.

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

Specify. McCann Worldwide (MRM). The Receiving Party shall not, without the Disclosing Party's prior written consent, disclose to any third party, any Confidential Information. The Receiving Party shall employ the same standard of care in protecting the Confidential Information as it would employ to protect its own confidential information, but shall in no event use less than reasonable care. The Receiving Party shall disseminate Confidential Information to its employees, agents and independent contractors only on a "need-to-know" basis. The Receiving Party shall cause each of its employees, agents and independent contractors who has access to Confidential Information to comply with the terms of this Section in the same manner as it is bound by this Section, with the Receiving Party remaining responsible for the actions and disclosures of any such employees, agents or independent contractors.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Reserve Officer Training Corps Program colleges.

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 recruiter must read the Privacy Act Statement to each person before collecting personal information letting them know that providing the information is voluntary however failure to provide recommended information could result in a denial of enlistment.

(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.

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

Once individuals consent to the collection of their PII the specific use is implied.

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.

Each form that a person fills out with their personally identifiable information has a privacy act statement incorporated into it in hard copy. The GO Army website has a privacy advisory on the opening page for information that is collected in electronic format.

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.