PRIVACY IMPACT ASSESSMENT (PIA)

For the

Standard Installation/Division Personnel System (SIDPERS) - Army National Guard (ARNG)
Army National Guard

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: 3894 / DA00108
- ☐ **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 007-21-01-20-02-2312-00

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 A0600-8-23 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. 05/03/2013

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; Army Regulation 600–8–23, Standard Installation/Division Personnel System Database Management; 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.

To support personnel management decisions concerning the selection, distribution and utilization of all personnel in military duties, strength accounting and manpower management, promotions, demotions, transfers, and other personnel actions essential to unit readiness; to identify and fulfill training needs; and to support automated interfaces with authorized information systems for pay, mobilization, and other statistical reports. The types of PII collected are personal, medical, employment, educational, and military information.

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

Access to data and data storage is controlled and accessible only to authorized personnel and authorized personnel with password capability for the electronic media access. Security perimeter protections are in place such as firewall, intrusion detection, and router access control list. Additionally, strict access control policies and procedures are implemented to ensure it is restricted only to those individuals with a need-to-know through role based access. The principal risk is incurred as information is collected and stored in the system and when information is extracted from the system and delivered outside the organization. The primary risk is human intervention resulting in the intended or unintended improper use of the information.

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. All Army components and major commands which includes Active, Army Accessions Command, Army Audit Agency, Army Cadet Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Inspectors General, Army Recruiting Command, Army Recruiting Information Support System, Army Reserve Command and to Commanders, Army Reserves, Army Training and Doctrine Command, Assistant Secretary of the Army (Financial Management & Comptroller) , Army Staff Principals in the chain of command, and Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service, Integrated Personnel and Pay System - Army, Defense Manpower Data Center, Department of Veterans Affairs, DoD Inspector General, Medical Command, National Guard Bureau, Office of the Secretary of Defense, Office of the Secretary of Defense Personnel and Readiness, and U.S. Military Entrance Processing Command.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. System is maintained with contractor support from Science Applications International Corporation (SAIC) in Arlington, VA.

All PII shall be:
- protected from loss and/or unauthorized disclosure.
- not be routinely processed or stored on mobile computing devices or removable electronic media without express consent of the SAIC AITS Program Manager.
- Transmitted via an encrypted mechanism. Transmitting PII records via email while unencrypted and via FTP while unencrypted is strictly forbidden.
- Restricted to the workplace when stored or processed on any mobile computing device (MCD). All MCDs must be encrypted using software approved by the SAIC Secondary Storage Device Encryption (SSDE) program.
- Delivered to SAIC from the Government using the GFI process.

☐ **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.

Service Members provide privacy information during their initial enlistment into the Army National Guard. If a Soldier declines to provide information, they are declined from entry into Service. Personal identifiable data retrieved from individuals is mandatory. Service members must provide information to this system for data to be accurate. The consent of use is most often in written format and must be declared by the Soldier of his/her own free will.

(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.

Soldiers maintain the option to choose whether or not their personal information be used for specific purposes. However, these objections could prevent the Soldier from receiving positive and/or negative personnel actions without the consent to use of the information. A service member may cooperate in providing all personal data with the exception of his/her SSN, ultimately this would prevent the enlistment as this is a unique identifier for each Soldier. Soldiers are presented with the Privacy Act of 1974 each time they are requesting services in the armed forces. This is a statement of rights, not an affirmation of consent. For each new instance the Soldier is provided a copy of the Privacy Act and a statement of consent outlining the uses of their personal information specific to the situation. Failure to provide consent by signing could result in a denial of services.

(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.

**The individual is provided a DD 1966 at the time of enlistment. On page 2 the "Privacy Act Statement" states the following:

PRIVACY ACT STATEMENT

AUTHORITY: Title 10 USC Sections 504, 505, 508, 12102; Title 14 USC Sections 351 and 632; Title 50 USC Appendix 451; and EO 9397 (SSAN).
PRINCIPAL PURPOSE(S): DD Form 1966 is the basic form used by all the Military Services and the Coast Guard for obtaining data used in determining eligibility of applicants and for establishing records
for those applicants who are accepted.

ROUTINE USE(S): None.

DISCLOSURE: Voluntary; however, failure to answer all questions on this form, except questions labeled as "Optional," may result in denial of your enlistment application.

**The individual is also provided with an informational "WARNING" on page 2 of the DD 1966. Below is the inclusive verbiage:

WARNING

Information provided by you on this form is FOR OFFICIAL USE ONLY and will be maintained and used in strict compliance with Federal laws and regulations. The information provided by you becomes the property of the United States Government, and it may be consulted throughout your military service career, particularly whenever either favorable or adverse administrative or disciplinary actions related to you are involved.