PRIVACY IMPACT ASSESSMENT (PIA)

For the

Drug and Alcohol Management Information System (DAMIS)

US Army Deputy Chief of Staff G-1, Headquarters

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: 2891/ DA00863
- ☐ **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 007-17-01-16-02-2496-00

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 A0600-85DAPE

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; 42 U.S.C. 290dd-2; Federal Drug Free Workplace Act of 1988; Army Regulation 600-85, Army Substance Abuse Program; and E.O. 9397 as amended (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.

DAMIS is a management tool which supports the The Army Center for Substance Abuse Programs (ACSAP). DAMIS is used to support the treatment, counseling, and rehabilitation of individuals who participate in the Army Substance Abuse Program. It identifies trends, judges the magnitude of drug and alcohol abuse, and measures the effectiveness of drug and alcohol prevention efforts in the Army. PII collect includes personal, medical, and military information.

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

Risks associated with the PII collected data is that they can potentially be used for financial gain if the information is compromised. We protect PII utilizing several security measures to lower the risks.

- Only Army Substance abuse program employees have access to this system. These users have varying degrees of access based on their job requirements and specific approval of the local Program Manager and ACSAP.
- Authentication – Users require authentication to access the PII data.
- Authorization – PII data is provided based on need to know basis.
- Firewall - The server resides in the Pentagon data center and is protected by a firewall that protects all the critical systems in the Pentagon data center.
- Encryption - Social Security Numbers are encrypted utilizing Oracle Database encryption. If a hacker did compromise the database, they would not be able to decipher the Social Security Number.
- Vulnerability Assessment – ACSAP frequently scans all servers to ensure discovery and patch of all vulnerabilities.

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 Duty, Army Accessions Command, Army Audit Agency, Army Cadet Command, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G-1, Army Intelligence and Security Command, Army Medical Department, Army Reserve Command, Army Training and Doctrine Command, Department of the Army Inspectors General, Provost Marshal General, Central Command, Installation Management Command, South Command, 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 Criminal Investigative Service, Defense Integrated Military Human Resources System, Defense Manpower Data Center, Defense Security Service, DoD Inspector General, Office of the Surgeon General, National Guard Bureau, Office of the DoD Inspector General, and the Office of the Secretary of Defense Personnel and Readiness.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. System Maintained by Akimeka , GINIA , and Pelatron.
The contractor assigned to this project will not require access to classified information. However, the ACSAP Software Application's contain highly sensitive data subject to protection by the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA). Contractor personnel will be required to pass a background check and sign written agreements controlling the release of information.

☐ **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.

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

Individuals are required to provide their information to receive substance abuse treatment services. Soldiers must verify their SSN information when providing a urine specimen for drug testing.

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.

Records that are stored can be used by the Army as allowed by law. However, records on an individual cannot be provided to outside agencies without the specific written consent of the individual.

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.

When an individual is screened by the counselor at the ASAP they are provided the Privacy act statement on DA Form 4465 as stated below:

PRIVACY ACT STATEMENT

AUTHORITY: 5 USC Section 301, Department Regulations; 10 USC Section 3013, secretary of the Army; 42 USC Section 290dd; Army Regulation 600-85, Army Substance Abuse Program (ASAP): and E.O. 9397

PRINCIPAL PURPOSE: Information is used to treat, counsel, and rehabilitate individuals who participate in the ASAP.

ROUTINE USES: The Patient Administration Division at the medical treatment facility with jurisdiction is responsible for the release of medical information to malpractice insurers in event of malpractice litigation or prospect thereof. Information is disclosed only to the following persons/agencies: to health care components of the Department of Veterans Affairs furnishing health care to veterans; to medical personnel to the extent necessary to meet a bonafide medical emergency; to qualified personnel conducting scientific research, audits or program evaluations, provided that a patient may not be identified in such reports, or his or her identity further disclosed by such personnel; upon the order of a court of competent jurisdiction.

DISCLOSURE: Mandatory for Active Duty service members. Failure to provide required information may be subjected to appropriate disciplinary action under the UCMJ. Voluntary for civilian employees, However, failure to provide all the requested information will prohibit processing comprehensive treatment.