PRIVACY IMPACT ASSESSMENT (PIA)

For the

PBANET - PINE BLUFF ARSENAL - UNCLASSIFIED ICAN

AMC - JMC - U.S. Army Joint Munitions Command

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: 3733 DA60212
- ☐ **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

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://dpcld.defense.gov/Privacy/SORNs.aspx

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.

* Primary authority is internal housekeeping. Used by personnel office to verify employment eligibility; by payroll office to set up direct deposit and process withholding; by security office for clearance actions; by health clinic for medical records.
* Civ Personnel/Acpers: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN).
* Civilian Pay (AF): 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. Chapter 53, 55, and 81; and E.O. 9397 (SSN).
* Civilian Pay (NAF): 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; E.O. 9397 as amended (SSN); & Army Regulation 215-3, Nonappropriated Funds & Related Activities Personnel Policies & Procedures.
* Military Pay: 5 U.S.C. 301, Departmental Regulations; 37 U.S.C., Pay and Allowances of the Uniformed Services; DoD Directive 5154.29, DoD Pay & Allowances Policy and Procedures; DoD 7000.14-R, DoD Financial Management Manual, Volume 7A, Military Pay Policy & Procedures – Active Duty & Reserve Pay; Joint Federal Travel Regulations (JFTR), Volume 1, "Uniformed Services Member," current edition; & E.O. 9397 (SSN), as amended.
* Badges: 10 U.S.C. 3013, Secretary of the Army; Army Regulation 190-13, The Army Physical Security Program & E.O. 9397 (SSN).
* Medical: 5 USC 552a, 29 CFR 1910.134 & TB MED 502; DLAM 100.2 para 2-1

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 PBANET is a small Directorate of Information Management (DOIM) managed network that combines such infrastructure components as routers, switches, hubs, and servers with few external connections to remote systems. PBANET supports local area network (LAN), wide area network (WAN) connectivity, and several local-unique PBA systems. It provides the mechanism for users to communicate via the Transmission Control Protocol/Internet Protocol (TCP/IP) over Ethernet. The PBANET must provide a network computing environment for all the Pine Bluff Arsenal users. PBANET will provide a network-computing environment, which is protected from network intrusion. This will lessen the number of systems and amount of information that is exposed to snooping, compromise, and theft from sources both within and outside of PBA through implementation of this system security design. Pine Bluff Arsenal is a member of the Army Material Command (AMC) and a subordinate to the Joint Munitions Command (JMC), Rock Island, IL. PBANET also supports tenant activities. The basic capabilities of the PBANET are: Provide high-speed network connectivity for official use only of all PBA automation resources via a single backbone. Provide centralized applications servers. Provide centralized file server. Provide centralized network management. Provide a single, centralized web page and web administration. Provide remote user support. NIPR CCSD's 7765, 7YQU.

Information stored on PBANET assets is considered Moderate Impact Category. The PII collected is used for common housekeeping tasks such as verifying employment eligibility, maintaining personnel records, security clearance verification, payroll & medical records. Also for determining whether access to post will be allowed by public for activities such as hunting & fishing. Any time PII is collected, sorted, shared or transmitted, there is risk it may be exposed, lost, or stolen, then used to cause harm.

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

Information stored on PBANET assets is considered Moderate Impact Category. The PII collected is used for common housekeeping tasks such as verifying employment eligibility, maintaining personnel records, security clearance verification, payroll & medical records. Also for determining whether access to post will be allowed by public for activities such as hunting & fishing. Any time PII is collected, sorted, shared or transmitted, there is risk it may be exposed, lost, or stolen, then used to cause harm.

Pine Bluff Arsenal (PBA) follows an established Incident Response Plan and procedures for marking, labeling, handling and disposing of PII data. All laptops and mobile devices are equipped with an approved Data-At-Rest solution. Permissions to electronic files are managed by the system administrator and limited only to those with need-to-know. Paper copies of PII are maintained in locked cabinets. PBA has taken steps to reduce the instances of Social Security Numbers on common forms as a method of employee identification.

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. Some Army components and major Commands including Joint Munitions Command, Army Materiel 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 Finance and Accounting Service

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

PII is required for payroll, clearance actions, access requests, access to government computer systems and information, and employment. The individual can object by telling the office requesting the information that they do not wish to provide the information. Typically, failure to provide the requested information may impede, delay, or prevent further processing of the action that has been desired by the individual.

(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 Privacy Act Statements describe the purpose/use of the PII. The individuals give their consent by

completing the form or by giving the information verbally to someone who is completing the form for them. They may withhold their consent by leaving the PII off the form they are completing, or by declining to give it to someone who is completing the form for them.

(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 Act Statements are formatted to include 4 sections: Authority, Principal Purpose, Routine Uses, & Disclosure. An example is given below from PBA Installation Access Badge Request, PBA Form 190-17. All Privacy Act Statements follow the format of having these 4 sections in this order:

AUTHORITY: 5 U.S.C. 5701, 5702, and E.O.9397 as amended (SSN)
PRINCIPAL PURPOSE(S): THE PURPOSE OF PBA ACCESS BADGE INFORMATION FORM IS TO ASSIST PINE BLUFF ARSENAL WITH THE PREPARATION OF PINE BLUFF ARSENAL ACCESS BADGES.
ROUTINE USES: THE ROUTINE USE OF THE PINE BLUFF ARSENAL ACCESS BADGE INFORMATION FORM IS TO PREPARE PINE BLUFF ARSENAL ACCESS BADGES, REPORTS OF NUMBERS, AND TYPES OF ACTIONS HANDLED BY THE PINE BLUFF ARSENAL PASS AND REGISTRATION OFFICE.
DISCLOSURE: VOLUNTARY DISCLOSURE. NON-DISCLOSURE MAY PRELUDE ISSUANCE OF A PINE BLUFF ARSENAL ACCESS BADGE.