PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automated Installation Entry (AIE) System

Joint Program Manager Guardian (JPMG)/Joint Product Manager, Force Protection Systems (JPM FPS), Headquarters Agency: Joint Program Executive Office for Chemical

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: DITPR #: 17221; (APMS: DA 304989)
- ☐ **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: AO-190-13-OPMG

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 0702-0125

Enter Expiration Date 01/31/2017

☐ **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 190-13, The Army Physical Security Program and E.O. 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.

In March 2001, the Chief of Staff, Army, directed all Army commanders to initiate access control at all installation entry points. The access control directive mandated relimination of installation entry related vulnerabilities, with the initial focus placed on gates, guards, and fences to channel traffic through installation access control points (ACP). In October 2003, the HQDA promulgated a new ACP policy stipulating 100 percent identification and verification of personnel entering the installation.

The focus of the AIE Program capability was initially to enhance the security at the installation's ACPs by automating authentication of authorized and registered personnel entering the installation. The goal of the AIE Program is to reduce the guard force requirements while maintaining or increasing personnel and vehicle throughput. The AIE enables adaptation of increased authentication requirements at increased threat levels. The capability primarily consists of integrated commercial off-the-shelf (COTS) products installed at Army installation ACPs. The AIE provides timely, effective, and efficient threat detection necessary for the installation commander to assess and react in all threat environments.

AIE enhances security through vetting and authentication of credentials, authorization of individuals, and establishing permissions to access Army installations. Data entry is registration, and for a permanent party, data entry harvests Common Access Card (CAC) information. For visitor control, data entry harvests driver's license information and issues passes. Authorized personnel will collect personal, military law enforcement and biometric information on individuals (with their consent) to populate the system's registration database. The installation database consists of a primary database connected to data entry, network management, law enforcement, a domain controller, and a variable number of gate servers for lane access control.

Data collected is used to enter personnel into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time, especially when the individual requires installation access. In the case of non-DoD individuals who require base access, an authorized visitor access pass (or equivalent) is produced. For prospective entrants who are not yet in the system database, individual credential data is automatically vetted through various DoD and National personnel databases. The records are maintained to support DoD and Army physical security, installation access, and information assurance programs, and provide installation commanders and law enforcement officials with means by which information may be accurately identified to determine if applicant meets authorized access requirements. Records stored in the AIE System are maintained to support Department of the Army physical security and information assurance programs and are used for identity verification purposes, to record personal data registered with the Department of the Army, and for producing installation management reports.

(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 safeguarding, we believe the risk to individuals' privacy to be minimal. Data is collected and employed in a dedicated security mode. Data sharing occurs only among individuals authorized access to the system as stated in the governing Privacy Act system notice. Data screens are marked with the "For Official Use Only" data handling legend. Privacy data is always encrypted when in transit among system components and outside of AIE, and is always stored in encrypted form. AIE employs FIPS-140-2 compliant encryption technology to protect all information (e.g., AES-256). This includes data while in-transit or at rest (e.g., IPSec-enabled protocol, Virtual Private Network (VPN) connections). AIE is also a self-contained system with known, limited, and encrypted interfaces within the AIE enterprise and beyond to preselected, trusted entities. All system users are made aware of restrictions on secondary use of the data by initial and refresher Privacy Act and Information Assurance training.

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. Information will be available to authorized users with a need-to-know in order to perform official government duties. These Component agencies may include HQDA and Army Staff Principals, Provost Marshal General (PMG), United States Army Inspector General (IG), Army Audit Agency (AAA), United States Criminal Investigation Command (USACIDC), US Army Intelligence and Security Command (INSCOM), and Assistant Secretary for the Army for Financial Management & Comptroller (ASA FM&C). Where installed at Joint Bases, maintaining perimeter security control will default to AIE.

☒ **Other DoD Components.**

Specify. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include the Defense Manpower Data Center, DoD Office of the Inspector General (OTIG), Defense Criminal Investigative Service(DCIS), and the Defense Intelligence Analysis Center (DIAC). In addition, the DoD blanket routine uses apply to this system, and user data is entered into the Defense Enrollment Eligibility and Reporting System (DEERS). Data may also be used by security offices to monitor individuals accessing DoD installations and/or facilities. Data may be viewed by or shared with civilian employees, military members, and contractors assigned to JPdM-FPS for AIE materiel development and technical support, by operators responsible for registering individuals into the database, by installation Access Control Point (ACP) personnel, and by installation law enforcement personnel.

☒ **Other Federal Agencies.**

Specify. External to DoD: Data may be provided to other Federal agencies under any of the DoD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/notices/blanket-uses.html.

☐ **State and Local Agencies.**

Specify.

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

Specify. BAE Systems, Inc.
CONFIDENTIALITY
Prior to receiving any Personally Identifiable Information (PII), the contractor shall sign a Nondisclosure document, agreeing to keep all PII strictly confidential, to protect the data at its designated classification level. In addition, the Contractor shall agree to return all data to the Government upon completion of the task, to include destroying all computer or other files relating to the PII data, regardless of media.

Information Assurance
The Army has categorized the AIE system as a Mission Assurance Category (MAC) level II and Classified Level as (CL) Sensitive, in accordance with DoDI 8510.01.

Transportability. The Enterprise server suite shall be transported in a fashion to protect Personal Identifiable Information (PII). The PII data is to be physically protected at all times in-transit. The contractor shall hand carry all of the Enterprise Server equipment to ensure security of the PII.

Privacy Act: Work on this project requires that personnel have access to Privacy Act

Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

☐ **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.

Personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement. Privacy Act Advisory Statements are displayed upon log-in to the system.

(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.

Failure to provide the requested information will result in the denial of an authorized access pass (or equivalent) and denial of entry to Army installations.