PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automated Installation Entry (AIE) System
Joint Program Manager Guardian (JPMG)/Product Manager, Force Protection Systems (PM FPS), Headquarters Agency: Joint Program Executive Office for Chemical and

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	11707 (APMS: DA 184658)
☐	**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

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 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 registration of all vehicles entering Army installations and elimination of installation entry related vulnerabilities. The initial focus was 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 and vehicles entering the installation.

The focus of the AIE Program capability is to enhance the security at the installation's ACPs by automating authentication of authorized and registered personnel and vehicles 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. The system also is electronically linked to an issued radio frequency identification (RFID) tag installed on properly registered vehicles. Data entry is registration, and for a permanent party, data entry harvests Common Access Card (CAC) information and issues RFID tags for vehicles. 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 and vehicular data 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. The records are maintained to support DoD and Army physical security, installation access, and information assurance programs and are used to identity and registered vehicle verification purposes and for producing facility management reports. To 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 and vehicle information 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. 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).

☒ **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. 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 PM-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. Infotec Systems Corporation.
3.3.34.1 Security and Privacy Protections. The AIE System shall provide for user authentication security, including strong authentication, non-repudiation, and personal identification, in accordance with Section 4 of DoDI 8500.1. Verification, administration and critical system setup and configuration functions in the system shall be protected from tampering by unauthorized users. If the system processes or stores information protected under the Privacy Act of 1974, the system shall conform to the notification and other requirements in accordance with the provisions of DoD Directive 5400.11. The system shall provide for protection of all Privacy Act protected data during transmission over any network and storage in any server and database. In addition, the system shall provide for protection of all Privacy Act protected data during transmission over any network and storage in any server and database.

3.3.34.2 AIE System Certification and Accreditation. The Contractor shall comply with the requirements of the DoD and the Department of the Army information assurance (IA) programs as defined by DoDI 8500.2 and AR 25-2 to achieve IA through defense-in-depth approach that supports the evolution of a net-centric environment.

☐ **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. 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.

(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 the individual consented to the collection of PII they have given implicit consent to the specific uses of their PII by providing an approved identification at the time of applying for registration to employ the system.

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, as required by 5 U.S.C. 552a (e) (3), are provided at the collection point. The statement provides the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond the denial of an authorized visitor access pass (or equivalent) and denial of access to the installation, the name and number of the Privacy Act system notice. The statement is included on paper, poster board, and electronic collection forms. The AIE Privacy Act Statement reads as follows:

AUTHORITY: Executive Order 9397 (SSN); Title 10 U.S.C. Section 3013; DoDD 8500.1

PRINCIPAL PURPOSE(S): To provide installation commanders and law enforcement officials with means by which information may be accurately identified to determine if applicant meets authorized access requirements. Use of SSN is required to make positive identification of an applicant. 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 and vehicle information registered with the Department of the Army, and for producing installation management reports. Employed by security officials to monitor individuals accessing Army installations. SSN. Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to Army installations.

ROUTINE USE(S): The "DOD Blanket Routine Uses" are set forth at the beginning of the Army compilation of systems of records notices.

DISCLOSURE: Voluntary; however, 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

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.