PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

AIE INC 3 V1 - AUTOMATED INSTALLATION ENTRY INCREMENT 3 VERSION 1

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

10/23/18

Program Manager, Terrestrial Sensors (PM TS)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [x] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Automated Installation Entry (AIE), which is installed at installation gates, is designed to leverage technology to increase security for Soldiers, Family Members, Department of Defense (DoD) civilian workforce, retirees, contract employees and guests of Army bases by electronically validating an individual's identification based upon information supplied at the time of AIE registration. When fully deployed, the system will increase the traffic flow at the gates and provide a means to verify one's identification by using a personal identification number during periods of increased force protection conditions. People registered in the program will be able to be granted access to the post through the identified AIE lanes by swiping their Department of Defense-issued identification card into the system card reader. The two existing increments of AIE are predominately the same from a technical aspect with the major delta being a difference in vendor software solutions.

The system was specifically configured so that visitors are authenticated by several methods of identification when they approach a base access control point. The information is then transferred to a data center, where it is analyzed against a trusted traveler database. Meanwhile, an on-site camera system is used to capture images of the visitor’s vehicle, as well as a visual of the visitor’s face. All elements of the security system are then formulated to provide the guard on duty with the most sufficient data to determine access.

This data collection instrument will collect the following information: name, current address, phone number, grade, Social Security Number (SSN), DoD ID Number, status, date and place of birth, weight, height, eye color, hair color, gender, passport number, country of citizenship, geographic and electronic home and work addresses and telephone numbers, marital status, fingerprints, photographs, and identification card issue and expiration dates.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

To meet access control standards in identity proofing, vetting, and access fitness determination as specified in DTM 09-012 and AR 190-13.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The individual implicitly consents to the capture and use of PII at the time of employment, commissioning, or enlistment in the Department of Defense, at which time, they are provided a privacy advisory. In the case of visitors, including relatives of active-duty soldiers, retirees, contractors conducting business on Army installations and others explicitly consent to collection of selected items of PII when seeking access to Army installations. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement will be displayed at each Pedestrian portal, vehicle lanes and at all registration portals. Other visitors may reject providing their PII but such actions will result in denial of access to Army Installations.

Forms containing SSNs must meet the DoD Acceptable Uses in reference to the SSN Reduction Plan in order to require the SSN. Individuals are provided with a Privacy Act Statement for applications requiring the SSN to validate their identity. Individuals must provide their personal address, personal e-mail in our applications as indicated by the referenced SORN. A contact phone number is required, but the individual has the option of which phone number to provide.

f. 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.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

(1) The AIE automated registration information technology systems will display the following:
YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.

BY USING THIS IS (WHICH INCLUDES ANY DEVICE ATTACHED TO THIS IS), YOU CONSENT TO THE FOLLOWING CONDITIONS:
THE USG ROUTINELY INTERCEPTS AND MONITORS COMMUNICATIONS ON THIS IS FOR PURPOSES INCLUDING, BUT NOT LIMITED TO, PENETRATION TESTING, COMSEC MONITORING, NETWORK OPERATIONS AND DEFENSE, PERSONNEL MISCONDUCT (PM), LAW ENFORCEMENT (LE), AND COUNTERINTELLIGENCE (CI) INVESTIGATIONS.

AT ANY TIME, THE USG MAY INSPECT AND SEIZE DATA STORED ON THIS IS.

COMMUNICATIONS USING, OR DATA STORED ON, THIS IS ARE NOT PRIVATE, ARE SUBJECT TO ROUTINE MONITORING, INTERCEPTION, AND SEARCH, AND MAY BE DISCLOSED OR USED FOR ANY USG AUTHORIZED PURPOSE.

THIS IS INCLUDES SECURITY MEASURES (E.G., AUTHENTICATION AND ACCESS CONTROLS) TO PROTECT USG INTERESTS--NOT FOR YOUR PERSONAL BENEFIT OR PRIVACY.

NOTWITHSTANDING THE ABOVE, USING THIS IS DOES NOT CONSTITUTE CONSENT TO PM, LE OR CI INVESTIGATIVE SEARCHING OR MONITORING OF THE CONTENT OF PRIVILEGED COMMUNICATIONS, OR WORK PRODUCT, RELATED TO PERSONAL REPRESENTATION OR SERVICES BY ATTORNEYS, PSYCHOTHERAPISTS, OR CLERGY, AND THEIR ASSISTANTS. SUCH COMMUNICATIONS AND WORK PRODUCT ARE PRIVATE AND CONFIDENTIAL. SEE USER AGREEMENT FOR DETAILS.

(2) The Privacy Act placards displayed at registration stations and pedestrian portals will include the following text.:

PRIVACY ACT STATEMENT, as required by 5 U.S.C. 552a (e) (3)

AUTHORITY: Title 10 U.S.C. Section 3013, Secretary of the Army; Army Regulation 190-13, The Army Physical Security Program and E.O. 9397 (SSN).

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): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: The DoD 'Blanket Routine Uses' also apply to this system of records.

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] 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 defaults to AlE.

☐ Other DoD Components	Specify.	Internal DoD agencies that would obtain access to Pll 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 PdM 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.	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.	AIE verifies state-issued credentials with individual Department of Motor Vehicles (DMV) databases. Once authorized by an individual state law enforcement authority, AIE uses the Law Enforcement Vetting (LEV) capability provided by Iberon, LLC to access the National Law Enforcement Telecommunications System (NLETS). The external NLETS vetting service accesses National Crime Information Center (NCIC) Interstate Identification Index (III), DMV, and local and out-of-state Law Enforcement information systems for identity vetting utilizing driver's license information.

☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Leidos, LLC 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. Cybersecurity The Army has categorized the AlE system under FIPS-199 and CNSSI 1253 as having the following security objective categorizations: (1) Confidentiality: Moderate (2) Integrity: Moderate (3) Availability: Moderate in accordance with DoDI 8500.01 and 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 PI I. 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 US Code, Section 552a (5 USC 552a) and all applicable agency rules and regulations. FAR privacy clauses and/or references are included in the AIE contract.
☒ Other *(e.g., commercial providers, colleges).*	Specify.	AIE uses Iberon, LLC, a third-party vendor, to access multi-state Law Enforcement and DMV databases through NLETS and adjudicate actual queries with a "pass/no pass" or "green/red" determination for installation access without transfer of detailed PII. In accordance with FBI Criminal Justice Information Systems (CJIS) Security Policy, security agreements with Iberon, LLC, ensure proper handling of PII and criminal history data.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- ☒ Individuals
- ☒ Existing DoD Information Systems
- ☒ Other Federal Information Systems
- ☒ Databases
- ☐ Commercial Systems

From the individual, Defense Manpower Data Center's (DMDC) Interoperability Layer Services (IoLS) and DEERS, Army records, FBI/NCIC and State DMV and criminal databases.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [ ] Website/E-Form
- [x] Other *(If Other, enter the information in the box below)*

The AIE system uses electronic input devices and screens that provide an interface between the user and the AIE System for collecting PII to include name, current address, phone number, rank/grade, Social Security Number (SSN), DoD ID Number, status, date and place of birth, weight, height, eye color, hair color, gender, passport number, country of citizenship, geographic and electronic home and work addresses and telephone numbers, marital status, fingerprints, photographs, and identification card issue and expiration dates. Additionally, optical recording devices are also employed to collect PII. Cameras read and record license plate number of the vehicles used by persons requesting access. The system also records video streaming of vehicles, their occupants and pedestrians which include facial and other physical details.

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier AO-190-13-OPMG

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 5.6, Item 120 (DAA-

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

KE6. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment. Retention 6 year after terminating an employee or contractor's employment must be authorized by Records Management and Declassification Agency (RMDA) or subsidiary agency.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 3013, Secretary of the Army; Army Regulation 190-13, The Army Physical Security Program, and E.O. 9397 (SSN).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0702-0125; Expiration Date: 01/31/2017 (Renewal request submitted; pending approval). 60 Day Notice, 29 Dec 2016; Doc Citation: 81 FR 95970.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[ ] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[X] Driver's License	[ ] Education Information	[ ] Emergency Contact
[ ] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[ ] Home/Cell Phone	[X] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[ ] Medical Information
[X] Military Records	[ ] Mother's Middle/Maiden Name	[X] Name(s)
[ ] Official Duty Address	[ ] Official Duty Telephone Phone	[X] Other ID Number
[X] Passport Information	[X] Personal E-mail Address	[X] Photo
[X] Place of Birth	[ ] Position/Title	[ ] Protected Health Information (PHI)[1]
[ ] Race/Ethnicity	[ ] Rank/Grade	[ ] Religious Preference
[ ] Records	[ ] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[ ] Work E-mail Address	[X] If Other, enter the information in the box below	

Weight, height, eye color, hair color, fingerprints, photographs, and identification card issue and expiration dates.
The system also includes vehicle information such as license plate state and number associated with Personal Information Record.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[ ] Yes [X] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The current SSN Justification is expired 2016; however, the memo is updated and being staffed for signature.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

AIE meets the SSN acceptable use case definitions for Law Enforcement, Credentialing, National Security,

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

6. Although the AIE System must collect SSNs, the System does not use the SSN locally for processing or maintaining personal information records. Instead, the AIE System relies on an Electronic Data Interchange Personal Identifier (EDIPI), also known as the DoD Identification Number, which is a unique ten (10) digit number assigned to a person's record specific to IoLS. When the authoritative data sources with which the AIE System interfaces for vetting and credential authentication eliminate the use of SSNs as primary identifiers, AIE will no longer collect SSNs.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [X] No

The system's SSN reduction or elimination strategy is contingent upon DoD law enforcement, credentialing, and physical access control policies. As long as Federal and State agencies with which AIE System must interface, continue to use the SSN as a primary identifier for tracking and reporting of individuals, the AIE System will be required to collect and use the SSN.

b. What is the PII confidentiality impact level[2]? [ ] Low [X] Moderate [ ] High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [x] Cipher Locks
- [x] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Command Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [x] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [x] Least Privilege Access
- [x] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [x] User Identification and Password
- [ ] Virtual Private Network (VPN)
- [ ] If Other, enter the information in the box below

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	DA307608
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	1836
[ ]	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	2/28/2018
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

RMF Scorecard: DoD Security Authorization Decision: AUTOMATED INSTALLATION ENTRY INCREMENT 3 VERSION 1 - System / Project Name: AUTOMATED INSTALLATION ENTRY INCREMENT 3 VERSION 1, DoD Componen: DoD Component: Army - System ID: Army - Package Type: Assess and Authorize - Type Authorization: Yes -Authorization Decision: Authorization to Operate (ATO) - Period Covered: Authorization Date Authorization: 27 Feb 2018 - Termination Date (ATD)- 27 Feb 2018 26 Feb 2021 -System Type: IS Enclave - dcm

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[ ] Yes [X] No

If "Yes," Enter UII _____ If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	LTC BEIRE D. CASTRO	(1) Title	Product Manager (PdM FPS)
(2) Organization	Product Manager, Force Protection Systems	(3) Work Telephone	703-704-2416
(4) DSN	654-2416	(5) E-mail address	beire.d.castro.mil@mail.mil
(6) Date of Review	15 Nov 2017	(7) Signature	CASTRO.BEIRE.DEJESUS.1069583748 Digitally signed by CASTRO.BEIRE.DEJESUS.1069583748 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=CASTRO.BEIRE.DEJESUS.1069583748 Date: 2017.11.15 09:41:04 -05'00'
b. Other Official ***(to be used at Component discretion)***	RICKY L. GRANT	(1) Title	Organizational ISSM
(2) Organization	Program Manager Terrestrial Sensors (PM TS)	(3) Work Telephone	703-704-9309
(4) DSN	654-9309	(5) E-mail address	ricky.l.grant.ctr@mail.mil
(6) Date of Review	11/15/17	(7) Signature	GRANT.RICKY.L.1025026957 Digitally signed by GRANT.RICKY.L.1025026957 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=CONTRACTOR, cn=GRANT.RICKY.L.1025026957 Date: 2017.11.15 15:08:28 -05'00'
c. Other Official *(to be used at Component discretion)*	SCOTT D. MACMILLAN	(1) Title	Program-ISSM
(2) Organization	Program Executive Office Intelligence Electronic Warfare & Sensors	(3) Work Telephone	443-861-7861
(4) DSN	848-7861	(5) E-mail address	scott.d.macmillan6.civ@mail.mil
(6) Date of Review	11/15/17	(7) Signature	MACMILLAN.SCOTT.DENNIS.1248274308 Digitally signed by MACMILLAN.SCOTT.DENNIS.1248274308 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=MACMILLAN.SCOTT.DENNIS.1248274308 Date: 2018.01.16 11:34:41 -05'00'
d. Component Privacy Officer (CPO)	Tracy C. Rogers	(1) Title	Chief Privacy Officer
(2) Organization	HQDA/OAA/RMDA/PA	(3) Work Telephone	571 515-0248
(4) DSN		(5) E-mail address	tracy.c.rogers2.civ@mail.mil
(6) Date of Review	10/10/18	(7) Signature	ROGERS.TRACY.C.1469542692 Digitally signed by ROGERS.TRACY.C.1469542692 Date: 2018.10.10 11:01:52 -04'00'

e. Component Records Officer	Anthony D. Crawley Gibson	(1) Title	United States Army Records Officer Chief, Records Management Division
(2) Organization	Records Management and Declassification Agency	(3) Work Telephone	703-428-6464
(4) DSN	328-6464	(5) E-mail address	anthony.d.crawley-gibson.civ@mail.mil
(6) Date of Review	06/12/18	(7) Signature	CRAWLEY-GIBSON.ANTHONY.DWAYNE.1043679801 Digitally signed by CRAWLEY-GIBSON.ANTHONY.DWAYNE.1043679801 Date: 2018.08.10 16:28:16 -04'00'
f. Component Senior Information Security Officer or Designee Name	Melissa C. Hicks	(1) Title	Acting, Chief, Cybersecurity Policy and Governance Division
(2) Organization	HQDA CIO/G-6, Cybersecurity and IA Directorate	(3) Work Telephone	703-545-1604
(4) DSN	865-1604	(5) E-mail address	Melissa.c.hicks.civ@mail.mil
(6) Date of Review:	10/23/18	(7) Signature	HICKS.MELISSA.C.1230666250 Digitally signed by HICKS.MELISSA.C.1230666250 Date: 2018.10.23 17:05:54 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Bruno C. Leuyer	(1) Title	Staff Director
(2) Organization	HQDA/OAA/AHS	(3) Work Telephone	571-515-0500
(4) DSN		(5) E-mail address	Bruno.c.leuyer.civ@mail.mil
(6) Date of Review	10/10/18	(7) Signature	LEUYER.BRUNO.C.1156265183 Digitally signed by LEUYER.BRUNO.C.1156265183 Date: 2018.10.10 14:22:12 -04'00'
h. Component CIO Reviewing Official Name	Carol M. Assi	(1) Title	Acting, Deputy Director
(2) Organization	HQDA CIO G-6, Cybersecurity & Information Assurance	(3) Work Telephone	703-545-1692
(4) DSN	865-1692	(5) E-mail address	Carol.m.assi.civ@mail.mil
(6) Date of Review	10/23/18	(7) Signature	HICKS.MELISSA.C.1230666250 Digitally signed by HICKS.MELISSA.C.1230666250 Date: 2018.10.23 17:07:10 -04'00'

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.