PRIVACY IMPACT ASSESSMENT (PIA)

For the

LENEL - LENEL ON GUARD

AMC - AMCOM - U.S. Army Aviation and Missile 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: (AITR: DA305705)
- ☐ **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 A0190-13 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;
Department of Defense Directive 8500.1, Information Assurance (IA);
DoD Instruction 8500.2, Information Assurance Implementation;
Army Regulation 25-1, Army Knowledge Management and Information Technology;
Army Regulation 25-2, Information Assurance;

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.

Lenel On Guard software allows the installation to fulfill security driven regulatory guidance with low manpower costs. This system allows security force personnel to monitor areas and facilities remotely therefore acting like a force multiplier.

Badge room personnel receive a AMLD 1137, LEAD Badge Record. From that form, data is entered into the application server using a PC with the application installed on it. The application server then stores the information at the database server.

Access information that is correlated with each badge number is stored at all of the local processors. Local processors are located at each facility where Physical Access Controls PACs are located. They are the memory for the PACs so the PACs don't have to communicate with the application server in order to work. Local processors get updated by the application server periodically. All that is stored at the local processor is name, badge number and whether or not the badge has access to any of the physical access controls connected to that particular server.

Information inputted into the system is as follows: Name, Directorate, Building number, Clearance Level, Areas of Access, Birth Date, Sex, Height, Weight, Eye Color, and Hair Color. There are addional fields with PII (such as phone number and address) but these are left blank.

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

Every system has the potential for information to become compromised and accessible by individuals without an official need-to-know, whether through conventional hacking techniques, lost media, or intentionally by an insider. Every individual who has access to the system, with regards to using the entered data, has undergone a security background review and privacy and security training. The LENEL ON GUARD application is maintained and only accessible by authorized personnel in positions of trust who have undergone a security background review and privacy and security training. These individuals are part of the installation security office and are responsible for verifying Letterkenny personnel clearances and authorization for access into LEAD facilities.

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. Used by our physical/personnel security office to verify access to Depot facilities

☐ **Other DoD Components.**

Specify.

☐ **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.

This is required for all personnel receiving un-escorted access to LEAD facilities and is part of their job. They can object to the collection of this information but it will establish reasonable grounds to not allow the individual access to the installation facilities.

(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.

This is required for all personnel receiving un-escorted access to LEAD facilities and is part of their job. They can object to the collection of this information but it will establish reasonable grounds to not allow the individual access to the installation facilities.

(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.

To receive their badge, LEAD personnel must complete a AMLD FORM 1137. On the form, the following is displayed.

Title of Form: LEAD employee/Contractor/Visitor Photo Record Card
Prescribing Directive: AMCR 190-3
Authority: USC 3012 Executive order 9397
Principal Purpose9s): Establish pertinent information in establishing positive description of identification, physical and photographic. Authenticate official requesting authorization for access to LEAD with picture badge. Routine Uses: Information to be utilized by Security Division Personnel to fabricate picture badges, key cards and establish areas of authorization, work site, home address and security classification required for continuous admittance to Letterkenny Army Depot. Mandatory or Voluntary Disclosure and Effect on Individual Not Providing Information Voluntary. Failure to disclose information may establish reasonable grounds for being denied access to this installation on a continuous basis without unreasonable delay. Privacy Act Statement - 26 Sep 75

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.