PRIVACY IMPACT ASSESSMENT (PIA)

For the

Employee Locator Force Protection (ELFP)
U.S. Army Aviation and Missile Life Cycle Management Command (AMCOM)

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: 9176 (AITR: DA147250)
- ☐ **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 A0500-3c G3/5/7 (DAMO)

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 OMB Control Number has been requested.*****NOTE: An OMB Control Number is not required for this system. See corrected SORN provided by Army Privacy. (LJ)

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.

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

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 Employee Locator Force Protection (ELFP) application hosted by the US Army Aviation and Missile Life Cycle Management Command (AMCOM LCMC) is a force protection measure that provides a central location for collecting and storing work and personal contact information. ELFP has two user interfaces.

(1) The Redstone Personnel Locator (RPL) is the employee interface to ELFP. RPL collects both work and personal contact information. Personal contact information is protected and only released to the employee's chain of command and the AMCOM Operations Center who has a need to know in time of emergency.

(2) The Employee Locator Database (ELD) is the manager's interface to ELFP. ELD is a management tool for employee accountability in case of a work place emergency. The ELD provides managers restricted access to their subordinate chain of command employee's work and personal contact information collected in RPL. Personal contact information may be used to contact employees during periods of national, local or personal emergencies. ELD does not collect PII information. The information is collected in RPL and stored in ELFP.

The type of Personally Identifiable Information (PII) is personal, employment, and work-related.

(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. There is a low risk that information may be accessed by unauthorized users through unauthorized access or network breaches; however, the ELFP website is protected by the use of Secure Sockets Layer (SSL) protocol, firewalls, antivirus software, and require Common Access Card (CAC) logon. Personal contact information is protected and only released to those in the employee's chain of command plus and the AMCOM Operations Center who has a need to know in time of emergency.

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. Internally to U.S. Army Aviation and Missile Life Cycle Management Command (AMCOM LCMC)

☐ **Other DoD Components.**

Specify. None

☐ **Other Federal Agencies.**

Specify. None

☐ **State and Local Agencies.**

Specify. None

☐ **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.

Individuals have the opportunity to object to the collection of PII by not utilizing the system. If the individual chooses not to voluntarily provide the information, it may prevent the individual from participating in the programs managed by the system. The individual consents to use by inputting the requested data. The posted Voluntary Information Disclosure Policy states the PII data collection is voluntary, why it is requested, how it will be used and to whom it may be released. The PII collected is used only for the specified purpose of 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.

Individuals have the opportunity to object to the collection of PII by not utilizing the system. If the individual chooses not to voluntarily provide the information, it may prevent the individual from participating in the programs managed by the system. The individual consents to use by inputting the requested data. The posted Voluntary Information Disclosure Policy states the PII data collection is voluntary, why it is requested, how it will be used and to whom it may be released. The PII collected is used only for the specified purpose of the system.

(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.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [x] **Other**
- [ ] **None**

Describe each applicable format.

Privacy and Security Notice

Thank you for visiting our product and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our product unless you choose to provide that information to us.

---

1. This product is provided with controlled access by the U.S. Army Aviation & Missile Command.

2. Information presented on this application / website is considered unclassified information and is accessed by authorized users unless otherwise specified. Use of appropriate byline / photo / image credits is requested.

3. For product management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. No user-identifying information is collected for this analysis. The information collected includes the following types of data:

a. Number of Hits for Home Page and Number of Successful Hits for Entire Product
b. Number of User Sessions (from United States and International) and Most Active Countries
c. Most and Least Requested Pages
d. Top Entry and Exit Pages
e. Single Access Pages and Number of Page Views
f. Most Downloaded Files
g. Most Submitted Forms and Scripts
h. Most Active Organizations or Companies that Accessed Product

4. For product security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with Army Aviation and Missile Command Records Administration Guidelines. All data collection activities are in strict accordance with DoD Directive 5240.1 (reference(p)).

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. The appearance of hyperlinks does not constitute endorsement by the Department of Defense, the U.S. Army, AMC, or the Army Aviation and Missile Command of the product or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare, and Recreation products, the Department of Defense or the U.S. Army does not exercise any editorial control over the information you may find at these locations.