PRIVACY IMPACT ASSESSMENT (PIA)

For the

AMC Emergency Notification System (AMCENS)
Army Materiel Command HQAMC

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:

- [x] **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?

- [x] **Yes, DITPR** Enter DITPR System Identification Number: 13926 (DA201664)
- [ ] **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**
- [x] **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.

- [x] **Yes**
- [ ] **No**

If "Yes," enter Privacy Act SORN Identifier A0025-1 CIO G6

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; AR-1, Army Knowledge Management Information Technology; Army Regulation 25-2, Information Assurance; 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.

HQAMC has identified the requirement to more efficiently communicate with and more easily account for civilian and military personnel and contractors during emergency and non-emergency situations across various geographical locations. AMC Emergency Notification System (AMCENS) allows for the identification of the location of employees/contractors/military personnel on duty status for emergency notification purposes and to manage home and contact information. Additionally, the system can assist in emergency situations to identify location of employees on non-duty status if the employee chooses to provide optional information. Each employee is expected to report his/her work status i.e. in office, telework, on TDY, etc.

The types of PII collected military, personal, employment, and work related information.

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

Risk: PII location
Mitigation: PII data is maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Facility is equipped with alarms, cameras, and personnel around the clock.

Risk: Electronic access via username/password
Mitigation: Users must authenticate against Army Knowledge Online directory and follow Army policy for changing passwords.

Risk: Electronic access to records
Mitigation: Access to records is limited to Person(s) with an official need to know who are responsible for servicing the record in performance of their official duties. Access to computerized data is role-based and further restricted by passwords, which are changed periodically.

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. U.S. Army Materiel Command (AMC) G1 Offices, G3/5 and individuals' own HR/Admin Office.

☐ **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.

Individuals objecting to the collection of PII may contact their MIRARS System Administrator who will provide alternatives that do not require the provision of PII.

(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.

The individuals' information is only being used for the notification process, and therefore no other uses apply.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

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

Describe each applicable format.

PRIVACY ACT STATEMENT

Authority: 10 U.S.C. 3013, Secretary of the Army and DoD Directive 3020.26,The Defense Continuity Program.

Purpose: To document names and phone numbers of persons to be notified in emergency situations.

Routine Use: None. The 'Blanket Routine Uses' apply.

Disclosure: Voluntary. Failure to supply this information may result in not being notified of a potential emergency to include acts of nature, accidents and technological and/or attack-related emergencies.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☒ Employment Information	☒ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Essential employee data will be collected from the MODERN database and the employees will be asked to complete the data collection themselves. Essential contractor information will be collected from each individual organization, and those workers would be asked to complete data in the system as well.