PRIVACY IMPACT ASSESSMENT (PIA)

For the

ASMIS-R - ARMY SAFETY MANAGEMENT INFORMATION SYSTEM - REVISED

US Army Combat Readiness(USACRC)

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: 2681 DA02695
- ☐ **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 A0385-10/40 ASO

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; 5 U.S.C. 7902, Safety Programs; Pub.L. 91-596, Occupational Safety and Health Act of 1970; DoD Instruction 6055.1, DoD Safety and Occupational Health Program; Army Regulations 385-10, Army Safety Program; Army Regulation 385-40, Accident Reporting and Records; 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.

Information will be used to monitor and facilitate the U.S. Army's and the USACE Safety and Occupational Health Offices' safety programs; to analyze accident experience and exposure information; to assimilate and analyze injury/illness information, to collect, verify, stage, & disseminate Safety and Occupational Health data, to identify trends and problem areas via data mining techniques and ad hoc analysis, to monitor recommended controls and logging hazards, and to provide preventive measures via risk assessments.

Type of PII: Personal, medical (injury/illness), employment, education, and mishap information.

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

Due to the stringent safeguards and access requirements the system and data are secure and it is unlikely the data would be compromised or provided to unauthorized or agencies. The risk associated with the collected data is unauthorized access. We address and mitigate (not negate) this risk by implementing the physical, technical, and administrative controls identified in SECTION 3, d.(1), d.(2), and d.(3).

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. US Army - due to this being an Army safety system, data is shared with all supervisors and manager in all Army organizations who have a need to know in order to effect safety considerations and concerns.

☒ **Other DoD Components.**

Specify. OSD, Defense Safety Enterprise System (DSES), MEDCOM, IG, DoD Law Enforcement and Veteran Administrations who have a need to know in order to effect safety considerations and concerns.

☒ **Other Federal Agencies.**

Specify. Department of Labor, Federal Aviation Agency, National Transportation Safety Board, and National Safety Council who have a need to know in order to effect safety considerations and concerns.

☒ **State and Local Agencies.**

Specify. Law enforcement

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Global Support Services; Section 6.2 of the contract specifies requirement for favorable security clearances and Section 6.3 mandates suitable DoDD 8570.01-M Information Assurance certifications for all contractors and CE (Computing Environment) certifications as well.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

Since data are not collected directly from individual Soldiers they are not provided either a Privacy Act Statement or a Privacy Advisory from ASMIS applications. However, Soldiers implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

Consent of specific use of PII is implied at the time of collection.

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.

Since data is not collected directly from individual Soldiers, they are not provided either a Privacy Act Statement or a Privacy Advisory from ASMIS applications. However, Soldiers implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which

time they are provided a Privacy Advisory.

Consent of specific use of PII is implied at the time of collection.

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.

PII is obtained via Information Systems.

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.