PRIVACY IMPACT ASSESSMENT (PIA)

For the

SIARS - SAFETY INCIDENT AUTOMATED REPORTING SYSTEM

AMC - TACOM - U.S. Army Tank-Automotive and Armaments 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: 15037 DA206032
- ☐ **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

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.

EXECUTIVE ORDER 12196

DoDI 6055.07, 6 June 2011, Accident Reporting and Recordkeeping

AR 385-10, Chpt. 3, 10June 2010, The Army Safety Program, Accident Reporting and Recordkeeping

Occupational Safety and Health Act of 1970

29 CFR Part 1904.7, OSHA Record Keeping Regulation

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.

UPDATE 10.9.2015 - System Name changed from Safety Intelex Automated Reporting System to Safety Incident Automated Reporting System. Name was changed to more accurately reflect the system capability (managing and tracking safety incidents). -- Stephanie Tice

This is an unmodified COTS product. AMC G1 and TACOM LCMC identified the (Intelex) capability as a potential Bridging Strategy to the future Material Enterprise and possible solution to the Army Combat Readiness/Safety Center as (1) A single solution for accident, incident (near miss), and work hazard tracking all soldier, civilian, and contractor accidents and injuries. (2) A potential 12 to 1 reduction in installation safety solutions (AWCF sites); (3) A streamlined data migration process to the Materiel Enterprise solution; (4) Intelex solution alignment with the ESOH requirement set; (5) Management Visibility through an authoritative data source for the Senior Leader Dashboard - Safety. With over 40 additional benefits, intelex modules / tools also provide a closed-loop process for performing, reporting on, and correcting hazards resulting from safety inspections. The system also provides both standard and customizable reports at multiple organizational levels that enables the Safety Offices, Commanders and Production Supervisors to evaluate safety performance across installations or within an installation. Intelex also provides a 'dashboard' view of safety for the installation/organization which provides leadership an easy to understand view of safety for their organization.

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

Privacy risks associated with SIARS are low due to the fact that limited PII will be collected. Risks are mitigated by requiring CAC authentication in addition to role based password access based on an official need-to-know. Every individual who has access to the system, with regards to using the entered data, has undergone a security background review, privacy and security training.

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. TACOM Life Cycle Management Command (LCMC) Installation Safety Offices, CECOM Life Cycle Management Command (LCMC) Installation Safety Offices

☐ **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.

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

Per 29 CFR Part 1904.7, employers are required to record any significant work-related injury or illness that is diagnosed by a physician or other licensed health care professional. Individuals at TACOM must provide all information on their respective clinic passes. (Differes by Location)

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.

Per 29 CFR Part 1904.7, employers are required to record any significant work-related injury or illness that is diagnosed by a physician or other licensed health care professional. Individuals at TACOM must provide all

information on their respective clinic passes.

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.

ANAD Form 40-3 or RRAD Form 601-E

SIARS Injury Report is a workflow that is completed by a supervisor when an employee is injured on the job which in-turn auto-populates a majority of the ANAD Form 40-3 or the RRAD 601-E clinic passes. They are then printed, signed by the supervisor, and taken to the clinic by the individual requiring treatment. Only a PORTION of the forms are auto-completed; the rest of the form is completed in person at the clinic, and never re-entered into SIARS. Both forms are attached, and the highlighted fields on each respective form are the fields that are auto-populated by SIARS.

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.