PRIVACY IMPACT ASSESSMENT (PIA)

For the

ENGLINK - ENGLink Interactive

US Army Corps of Engineers

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: 2955/ DA05111
- ☐ **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 202-000001020

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 submitted to Army Privacy on 3/20/2017 (new SORN, no #)

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; 33 U.S.C 701n, Emergency Response to Natural Disasters; 42 U.S.C 5121; Congressional Findings And Declaration; ER 690-1-321, Staffing for Civilian Support to Emergency Operations

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.

Engineers Link Interactive (ENGLink) is the U.S. Army Corps of Engineers (USACE) command and control system emergency management automated information system. ENGLink provides the framework for processing information and performing command and control of USACE elements responding to civil and military contingencies. ENGLink represents "ground truth" reporting and allows deployed personnel real-time access to critical information. The ENGLink system represents a single data entry point that standardizes and integrates methods of collecting, analyzing, forecasting, and presenting information for decision makers. The system compiles reports from data entered at the site of an emergency operation and from other responding elements in the organization's chain of command.

ENGLink is a role-based application tied to USACE's Userid-Password Administration and Security System (U-PASS). Only employees with valid user accounts and assigned U-PASS user capabilities can access the information system based on permission parameters. Once inside the ENGLink application, users can only access information that is within their permission parameters. Furthermore, ENGLink is HIPAA and CAC enforced, ACE-IT provides all communication channel controls, configuration and security technology including Key Management and Token and Certificate standards (PKI).

Types of information collected:
Name(s), home address(es), phone number(s), driver's license, government passport information, medical information, and email addresses

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

ENGLink captures/contains/processes PII to facilitate emergency response services. The information stored in the ENGLink database allows managers to find qualified and available staff. The information is used to permit the location and deployment of staff to mission sites. The deployed personnel section tracks details of the employees' assignments that can be briefed using the capabilities of the reporting module. Information about federal employees and military personnel is collected and stored in the Oracle database which provides a "medical clearance" score and determines whether or not the individual is "fit" to deploy to a disaster site and under what conditions they may deploy.
USACE employees, contractors, and military personnel have the option to submit to receive their "medical clearance" through the ENGLink application. This individually identifiable health information (IIHI) is stored in a 192-bit encryption hash using Oracle's Advanced Security features and Fine-Grained Access Control. This resulting data is not presented to any USACE, federal, or military employee, or contractors. The resulting "medical clearance" is used only to help identify qualified candidates for deployment and is viewed exclusively by USACE nurses and the WOHA (Washington Occupational Health Administration) staff, who reviews and processes medical clearances for USACE.

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. USACE

☐ **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. Contractor is required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

☐ **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.

PII is required for response and recovery CONUS/OCONUS deployments.

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.

Users are provided with a disclosure statement which has to be reviewed and acknowledged prior to gaining authentication authority. ENGLink also requires HIPAA and PII AUP (Acceptable User Policy) training via U-PASS (Userid-Password Administration and Security 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.

☒	**Privacy Act Statement**	☒	**Privacy Advisory**
☒	**Other**	☐	**None**

Describe each applicable format.

ACCEPTABLE USE POLICY (AUP): Web-based policy required for U-PASS authentication capabilities

CAC Registration/Authentication: Certificates are stored in CAC

PRIVACY ACT NOTICE: Pop-up before users access their "Personal Data Sheet"

PRIVACY DISCLAIMER: For all users

HIPAA Certification Test: Required only for users who need access to medical deployment record(s)
*****
Privacy Act Notice

Authority: 10 U.S.C 3013, Secretary of the Army; 33 U.S.C 701n, Emergency Response to Natural Disasters; 42 U.S.C 5121; Congressional Findings And Declaration; ER 690-1-321, Staffing for Civilian Support to Emergency Operations

The purpose for collecting information in the Medical Data Sheet (MDS) is to allow the Medical provider to review your medical condition to ensure that you can perform the job tasks assigned while working long hours, under stressful and sometimes physically demanding conditions without jeopardizing your health. Emergency Managers will use the Medical provider clearance determination to assign tasks and manage staff during deployment to emergency events. Providing information in the MDS is strictly voluntary. If you fail to provide the information the Medical provider will not be able to evaluate your medical condition and you may not be selected for deployment. I understand that omitting or providing inaccurate medical information may result in my not being selected for deployment, being returned to my home station prior to my task order ending, and being ineligible for future deployments.