PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

ENGLINK - ENGLink Interactive

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

09/09/20

US Army Corps of Engineers

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and 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 compliant and CAC enforced, USACE CIO/G-6 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, protected health information and email addresses

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

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.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII is required for response and recovery CONUS/OCONUS deployments however, if they object, they cannot be considered for deployment as they will not be listed in the ENGLink for selection purposes.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

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)

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [X] Privacy Advisory [ ] Not Applicable

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	USACE
[ ]	Other DoD Components	Specify.	
[ ]	Other Federal Agencies	Specify.	
[ ]	State and Local Agencies	Specify.	
[X]	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	General Dynamics Information Technology (GDIT) 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. FAR Clauses are in the contract.
[ ]	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [x] Individuals
- [ ] Databases
- [ ] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [x] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

ENG Form 6195

k. 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 must be consistent.

[x] Yes [ ] No

If "Yes," enter SORN System Identifier submitted to Army Privacy on 3/20/2017 (

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-AU-02-21

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

RN 500-3b1 - PERMANENT. TP. Keep in CFA until no longer needed for conducting business, then retire to RHA/AEA. The RHA/AEA will transfer to the National Archives when records are 30 years old.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must 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

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.