PRIVACY IMPACT ASSESSMENT (PIA)

For the

EDW - Enterprise Data Warehouse

U.S. Army Corps of Engineers - USACE

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: 10104 DA182404
- ☐ **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 202-00-03-00-01-1017-00-304-103

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 (New) Enterprise Data Warehouse (resubmitted 02 Mar 2017)

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;
USACE CIO Policy Memorandum 14-010, USACE Application Rationalization and Software Management, 13 April 2015;
USACE Campaign Plan FY15-19 Goal 4c: Streamline USACE Business, Acquisition and Governance Processes;
USACE CIO Priority #8 Optimize Infrastructure/Information and #10 Refine IT Investment Compliance.

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.

As a one-stop data service, business intelligence service provider, the Enterprise Data Warehouse (EDW) will pull information from various USACE systems, and provide access to data at a centralized location to the USACE Enterprise via the USACE Intranet. The EDW's primary role is to function as the central repository of shared data from which management reporting is accomplished. Currently the EDW contains a functionally defined subset of data from the following source systems: Automated Personal Property Management System (APPMS), Rental Facilities Management Information System (RFMIS), Operations & Maintenance Business Info Link (OMBIL), Integrated Manning Document (IMD), Human Resources, Dredging Information Systems (DIS), Locks Performance Monitoring Systems (LPMS), Corporate Records Management System (CRMS), Housing AP Management Information System (HAPMIS), Real Estate Management Information System (REMIS), Real Estate Corporate Information System (RECIS), Project Management Information System (P2), Facilities & Equipment Maintenance (FEM), Real Property Inventory (RPI), and U.S. Army Corps of Engineers Financial Management System (CEFMS) FY06 to CY.

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

As with any PII there are privacy risks associated with its use. However, the EDW has specific access controls so that only those who have been granted access can view the PII. In order to get this level of access a user must first be given USACE network access and then apply for EDW access. To get network access requires that the user have a background investigation as well as pass the USACE Command Information Assurance course designed to ensure users understand the legal and practical ramifications of the data they have access to. Additionally, the user has to sign and adhere to the Acceptable Use Policy (AUP). Any change in status or the termination of an employee or independent contractor with access will immediately result in the termination of the user's access to all systems where the PII may reside. Currently PII is collected from CEFMS, REMIS, HAPMIS, and IMD, which consists of Name, Race/Ethnicity, Gender, Education, Employment Information, Spouse Information, Home Telephone Number, Personal Email Address, Truncated SSN and Mailing/Home Address.

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. Only users with USACE network accounts with EDW access will have any access to the PII found in the EDW.

☐ **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. Various USACE contractors have access to the EDW based on their existing

contracts to support information systems. Every contractor with access to the EDW has taken multiple Information Assurance training classes aimed at informing them of their responsibilities with respect to handling the PII they will come in to contact with. Each of them has signed Non-Disclosure forms as well as formally acknowledged the responsibility given them by signing their Network Access forms.

☐ **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.

The EDW does not create the PII, it simply collects data from existing systems. This information is required in order to maintain the traceability of a record throughout its lifecycle. EDW functionality requires reference to responsible employee across multiple reporting applications.

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 EDW does not create the PII, it simply collects data from existing systems. This information is required in order to maintain the traceability of a record throughout it's lifecycle. EDW functionality requires reference to responsible employee across multiple reporting applications.

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.

The EDW does not create any PII, it simply collects data gathered from existing systems. All notifications are applied at the source system level.

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.