PRIVACY IMPACT ASSESSMENT (PIA)

For the

CWBI - CIVIL WORKS BUSINESS INTELLIGENCE

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: 3702/ DA05060
- ☐ **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 202-00-01-02-01-1031-00

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 A0015-2-2 CE (A1130-2-550b CE new number) and A1145b CE

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. 30 April 2015

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 OMB No. 0710-0003

Enter Expiration Date in progress (April 2016)

☐ **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.

Regulatory authority: Rivers and Harbors Acts of 1890 (superseded) and 1899 (33 U.S.C. 401, et seq.); Section 10 (33 U.S.C. 403).

Recreation authority:
Debt Collection Improvement Act of 1996, 31 U.S.C. 7701(c)
Title 36, Chapter III, CFR 327- Rules and Regulations Governing Public Use Of Water Resources Development Projects administered by the Chief of Engineers Executive Order 9397

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.

CWBI directly supports the Corps of Engineers Civil Works in the area of performance measures for Water Resources by consolidating, integrating, and displaying geospatial data in the business areas of Navigation, Environmental Stewardship, Safety, Recreation, Hydropower, Flood Risk Management, and Regulatory and providing one-time, single point data entry for these systems. The system includes a data warehouse that merges financial data with the business function output and inventory data to produce performance measures of efficiency and effectiveness for the Operations and Maintenance community. Life-cycle phase is mixed operations and maintenance; system program manager is Dr. Mark F. Sudol, Navigation and Civil Works Decision Support Center, Institute for Water Resources; functional proponents are James R. Hannon, HQUSACE Chief of Operations and Regulatory and James Dalton, Chief of Engineering at USACE. CWBI databases are located on servers at the two processing centers within the USACE Enterprise Infrastructure Services (ACE-IT) network. CWBI data tables are not directly linked to other USACE data tables for data sharing although data is uploaded to and/or extracted from other USACE data tables; CWBI does not interconnect with any system outside the ACE-IT production environment. System backup is provided by ACE-IT using servers located at the processing centers.

The Recreation module in the database includes the following primary personal information: individual's name, height, weight, eye color, date of birth, drivers license number, social security number, telephone number, and vehicle information: tag number, year, make, and color. The source of this information is directly from the individual record subject.

The Regulatory database includes the following primary personal information: individual's name, address, telephone number, fax number, and email address. The source of this information is directly from the individual record subject, a member of the public.

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

Any user accessing any Corps hardware, software or firmware, must have their Common Access Card (CAC) and a userid validated and maintained through the USACE User-ID Password Administration and Security System (UPASS) system. Any CWBI user must also be granted permission and then authenticated through the Oracle database. Passwords for both network access and database access must be changed every 60 days. The CWBI system administrator must also change the Oracle CWBI passwords every 60 days. Each user is provided a role that assigns the minimum access that the user needs. Users of CWBI are government employees and contractors. Users are not required to possess a security clearance for system access and Foreign Nationals employed by USACE may access CWBI. All persons accessing CWBI participate in a periodic security training and awareness program. All personnel with management responsibility are aware of operational and security-related procedures and risks. All personnel designated as ADP I, II or III are subjected to a pre employment background investigation. User access is terminated when a user no longer requires access. Users are required to lock their computers when leaving their workstations unattended. Passwords are inhibited, overprinted or otherwise protected from unauthorized observation on terminals and video displays. Passwords for systems processing must be at least an fifteen character string using the 36 alphabetic-numeric characters and do not need to be randomly generated. At least two of the characters must be upper case alpha, lower case alpha, numeric and special characters. User logon-restricted access is monitored for unsuccessful user logon after three attempts, privileged user logon/access, and directory/file access. After three unsuccessful user logons, the userid is blocked from subsequent attempts. Regular applied patches to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's) prevent any new opportunities to compromise CWBI data. Partners are provided information through regularly scheduled file transfers accomplished via ftp or email across the RSN or Non-classified but Sensitive Internet Protocol Router Network (NIPRNET). Files transferred across the Internet/NIPRNET are encrypted using a Virtual Private Network (VPN) or Advanced Encryption Standard (AES) 256-bit encryption.

Physical security consists of an access restricted area where the maintained server platforms are environmentally controlled and uninterruptible power supply protected. CWBI data is Unclassified-Sensitive Two (US2).

Security measures are tested annually.

Information is protected by firewalls, antivirus software, CAC UBE and data-at-rest protection software on portable laptops.

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.

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Regulatory data will be shared among state regulatory agencies to enable processing of joint federal and state permit applications.

☒ **State and Local Agencies.**

Specify. Recreation data will be shared with local law enforcement agencies.

Regulatory data will be shared among state regulatory agencies to enable processing of joint federal and state permit applications.

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

Specify. Standard contract language should be contained in the contracts; however, as contracts are renewed the new standard statement per DoD memorandum "DoD Component Responsibility to Ensure Government Contract Compliance with the Privacy Act" (28 JAN 2015) shall replace current statements.

☐ **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.

Recreation and Safety: Personal data is voluntarily given by the applicant and collected via manual forms.

Regulatory: Personal data is voluntarily given by the applicant and collected via electronic forms on the Internet Accessible segment of the USACE network or manual forms submitted to the district USACE Regulatory office. The ePermit form contains an applicable privacy statement.

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

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.

Recreation and Safety: Personal data is voluntarily given by the applicant and collected via manual forms.

Regulatory: Personal data is voluntarily given by the applicant and collected via electronic forms on the Internet Accessible segment of the USACE network or manual forms submitted to the district USACE Regulatory office. The ePermit form contains an applicable privacy statement.

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.

Recreation: Individual is presented with a citation, ENG 4381, that has the Privacy Act Statement on the reverse side. This is a Title 36 citation authority under Flood Act of 1970, Public Law 91-611.

Regulatory: Individual voluntarily fills out the ENG 4345 standard form that has the Privacy Act Statement on the face of the form. Form is approved by OMB No. 0710-0003.