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:

CWBI - CIVIL WORKS BUSINESS INTELLIGENCE

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

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.)*

- [x] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [ ] 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.

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. CWBI databases are located on servers at the two processing centers within the USACE Enterprise Infrastructure Services (CIO/G6) 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 CIO/G6 production environment. System backup is provided by CIO/G6 using servers located at the processing centers.

The Recreation module in the database includes the following primary personal information: individual's name, address, and vehicle information: tag number, make, model, body style, 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.

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)*

Recreation: Park rangers use the recreation module to collect data about the citations they issue to the public for misuse of Corps recreation areas.

Regulatory: The Mission of the Regulatory system is to assist in the processing of permit applications from individuals in order to allow reasonable development while protecting the Nation's waters and wetlands.

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.

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.

f. 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.

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.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

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.

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

☒ Within the DoD Component	Specify.	USACE Regulatory Permit team has access to the regulatory information. USACE Recreation team has access to the citation information.
☐ 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 *(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.	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. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

The source of the PII is from the individual for both the Recreation collection and the Regulatory collection.

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

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

Recreation: personal information is provided by the individual record subject via personal interview. ((ENG FORM 4381, MAR 2015 (EP 1130-2-550))

Regulatory: provided by the individual record subject by telephone interview or completion of electronic form (https://www.publications.usace.army.mil/Portals/76/Publications/EngineerForms/Eng_Form_4345_2018May.pdf)

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 A0015-2-2 CE and A1145b CE; currentl

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.

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

(3) Retention Instructions.

Record Series 400: Information Management 400B Information Management, Military Publications, Temporary Keep 0 - 6 years based on the Disposition Instructions.

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.

Regulatory authority: Rivers and Harbors Acts of 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

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.

[X] 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.

Form 4345 Application for a Department of the Army Permit U.S. Army Corps of Engineers (USACE) APPLICATION FOR DEPARTMENT OF THE ARMY PERMIT 33 CFR 325. The proponent agency is CECW-CO-R. Form Approved - OMB No. 0710-0003 Expires: 02-28-2022

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☐ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☐ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☐ Employment Information	☐ Financial Information	☐ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☐ Social Security Number (SSN) *(Full or in any form)*
☐ Work E-mail Address	☒ If Other, enter the information in the box below	

The Recreation module in the database includes the following primary personal information: individual's name, address, and vehicle information: tag number, year, make, model, body style, 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.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☐ No

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [ ] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

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).

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [ ] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

User access to all Corps hardware, software or firmware, must have a Common Access Card (CAC) and a userid validated and maintained through the USACE UPASS system. CWBI users must be granted permission and then authenticated through the Oracle database (DB). Passwords for both network/DB access must be changed every 60 days. The CWBI system admin must change the Oracle CWBI passwords every 60 days. Each user is provided a role that assigns the minimum access that the user needs. CWBI users are GOV employees and CTR. Users are not required to possess a security clearance for system access. 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 preemployment 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 a 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 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.