

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:

CWIFP APPLICATION SYSTEM - CORPS WATER INFRASTRUCTURE FINANCING PROGRAM APPLICATION SYSTEM

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

Corps of Engineers

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- | | |
|---|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees |
| <input checked="" type="checkbox"/> from both members of the general public and Federal employees | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input checked="" type="checkbox"/> New Electronic Collection |
| <input type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

The Corps Water Infrastructure Financing Program (CWIFP) application system is used to securely collect information needed by the U.S. Army Corps of Engineers (USACE) to evaluate the eligibility and suitability of prospective borrowers who request CWIFP credit assistance. It is used by the USACE CWIFP team and prospective borrowers (non-federal entities, cities, counties, states, and private entities) to submit applications. The system collects data to assess creditworthiness, identify project risks, negotiate credit terms, and determine budget requirements. It also stores and tracks loan application data, provides workflow support for application packages, and archives completed packages.

PII collected: Official Duty Address, Work E-mail, Official Duty Telephone, Position/Title, DoD ID Number, Name(s), Other ID Number (Unique Entity Identifier (UEI), Business Tax Payer ID, employer identification number).

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)

PII is collected for identification, verification, and administrative uses.

e. Do individuals have the opportunity to object to the collection of their PII? 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 collected for identification, verification, and administrative uses.

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.

By providing their information, individuals consent to the sharing of their information with the USACE CWIFP team to review and process the application. Personally Identifiable Information will not be shared outside the USACE CWIFP team. They are permitted to withhold their information, however incomplete submissions may delay or disqualify the project.

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.)

- | | | |
|--|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory | <input type="checkbox"/> Not Applicable |
|--|--|---|

Authority: Pub. L. 113-121 5001-5035, Water Resources Reform and Development Act of 2014; Water Infrastructure Finance and Innovation Act of 2014 (WIFIA, 33 U.S.C. 3901-3914).

Principal Purpose: The preliminary application will address the CWIFP eligibility criteria, CWIFP selection criteria, and identifies other specific information that must be provided to USACE to be considered for credit assistance. This serves to provide USACE with sufficient information to make a project selection and invite prospective borrowers to submit applications. The full application will provide USACE with information to assess the creditworthiness of both the applicant and project, identify the project's engineering and financial risk, negotiate the terms and conditions of the credit assistance, and calculate the amount of budget authority that will be needed to fund the project(s).

Routine Uses: Information will be shared with the USACE Corps Water Infrastructure Financing Program (CWIFP) team to review and process the application. Personally Identifiable Information will not be shared outside the USACE CWIFP team.

Disclosure: Voluntary, however incomplete submissions may delay or disqualify the project.

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

- | | | |
|---|----------|---|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | USACE CWIFP |
| <input type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. | |
| <input checked="" type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. | Environmental Protection Agency |
| <input checked="" type="checkbox"/> State and Local Agencies | Specify. | State/local governments, tribal governments, corporations, trusts, joint ventures, or state infrastructure financing authorities. |
| <input checked="" type="checkbox"/> 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. | Contractor TBD. |
| <input type="checkbox"/> 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)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

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

- | | |
|---|---|
| <input type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

ENG 6177 - Corps Water Infrastructure Financing Program Application

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.

- Yes No

If "Yes," enter SORN System Identifier

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

Not retrieving by personal identifier.

I. 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.

GRS 1.1 items 10 and 11

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

(3) Retention Instructions.

GRS 1.1 item 10: DAA-GRS-2013-0003-0001, Temporary: Destroy when 6 years after final payment or cancellation, but longer retention is authorized if needed for business use. GRS 1.1 item 11: DAA-GRS-2013-0013-0002: Temporary: Destroy when business use ceases.

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 statute 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.

Pub. L. 113-121 5001-5035, Water Resources Reform and Development Act of 2014; Water Infrastructure Finance and Innovation Act of 2014 (WIFIA, 33 U.S.C. 3901-3914).

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.

OMB 0710-0026, Corps Water Infrastructure Financing Program (CWIFP) Applications. Expires: 08/31/2026

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)

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

Other ID: Unique Entity Identifier (UEI), Business Tax Payer ID.
 Public (state/local governments, tribal governments, corporations, trusts, joint ventures, or state infrastructure financing authorities):
 borrower name, business phone and mailing address, employer identification number, and Unique Entity Identifier (UEI).

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 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 level²? Low Moderate High

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

²Guidance 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

c. How will the PII be secured?

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

- | | |
|---|--|
| <input type="checkbox"/> Cipher Locks | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> If Other, enter the information in the box below |

Physical Controls for the data center are inherited from Microsoft Azure. Main access to Azure datacenter facilities is restricted to a single point of entry that is manned 24x7 by security personnel. Emergency exits are alarmed and under video surveillance. Electronic access control devices are installed on doors separating the reception area from the facilities' interior to restrict access to approved personnel only. Azure datacenters have a security operations desk located in the reception area and in line of sight of the single-entry point. The datacenter lobbies have man-trap portal devices that require access card and biometric hand geometry or fingerprint authentication to pass beyond the lobby. Areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, MDF rooms, etc.) are further restricted through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Additionally, doors are alarmed and under video surveillance.

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

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

Backups are maintained by Microsoft through Azure Backup (subscription-based service) and/or Azure data center Disaster Recovery (DR) procedures. Azure backup extends traditional backup tools on premise with tools in the cloud. Backup allows the protection of data from customer datacenters, remove and branch offices, and cloud applications using on premise and cloud storage. For disaster recovery (DR) purposes, Azure keeps customer data durable in two locations with the customer having the capability to choose the location of the backup site. In both locations, Azure constantly maintains multiple healthy replicas of customer data. Azure/O365 data is replicated through FIPS 140-2 compliant TLS 1.2 secure channels to protect the confidentiality, integrity, and availability of the information.

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

- | | | |
|---|---|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Common Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input checked="" type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input checked="" type="checkbox"/> Least Privilege Access |
| <input checked="" type="checkbox"/> Role-Based Access Controls | <input checked="" type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input type="checkbox"/> User Identification and Password |
| <input checked="" type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> If Other, enter the information in the box below | |

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

For identity and authentication, there will be two Enterprise IDAM solutions, one for Army users (including USACE), and a secondary one for external users. This strategy will separate credentials, and allow USACE to manage their external users in a separate directory.