



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Manning Document (IMD)

Headquarters, US Army Corps of Engineers (HQ 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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN).

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.

The Integrated Manning Document (IMD) is a custom-designed, comprehensive USACE enterprise manpower management system. The IMD is a web-based editing, report and query system to be used by USACE manpower analysts at the activity level to maintain current position data on all USACE civilian, uniformed personnel, Contractors, Foreign Nationals and Interns. The IMD database is being used by Headquarters, USACE and the USACE field to maintain local manning information as well as to provide specific information necessary in managing the manpower strength in support of USACE and its mission.

The IMD provides to any authorized user a real-time view of all positions whether filled or under recruitment and all organizational elements in USACE. This information is used as a building block for effective centralized and regional recruitment and training programs and as a strategic tool by the Regional Management Boards and Commanders.

The requirement is to conduct manpower management, validate requirements, authorizations and actual positions/personnel. USACE collects information from the Defense Civilian Personnel Data System (DCPDS), reviews, verifies and updates USACE IMD database bi-monthly. HQ USACE generates upward reporting in support of USACE.

Type of PII collected, name, grade/rank, salary, SSN last four positions, security clearance, education and citizenship.

MIS is the predecessor of what is now the IMD process.

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

Privacy risk would be unauthorized access/release of PII data fields. To mitigate these risks, computerized records are maintained in a controlled area accessible only to authorized personnel. Entry is restricted by the use of locks, guards and administrative procedures. Access to personal information is limited to those who require the records in the performance of their official duties and to the individuals who are the subjects of the record or their authorized representatives. Access to personal information is further restricted by the use of unique logon and passwords, which are changed according to USACE password policy. This system has a current ATO. The system resides on secure Army and Federal government facilities (Vicksburg, MS and Portland, OR). Physical records are stored on USACE servers at WPC/CPC with standard security protections.

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.

State and Local Agencies.

Specify.

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

Specify.

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.

Information is being retrieved from another data collection instrument (DCPDS); this information is required for USACE to have a position management system that can be updated electronically in order to comply with IG directives. Being in DCPDS is required for employment.

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.

Information is being retrieved from another data collection instrument (DCPDS): this information is required for USACE to have a position management system that can be updated electronically in order to comply with IG directives. Being in DCPDS is required for employment.

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.

Data is retrieved from the Defense Civilian Personnel Data System (DCPDS), another DoD IT system.

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.