



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Privacy Act Workflow System (PAWS)

DoD Consolidated Adjudications Facility

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
- 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

Pending

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.

Authority to collect this information is contained in 5 U.S.C. § 552a, the Privacy Act of 1974, as amended; 10 U.S.C. 113, Secretary of Defense; 32 C.F.R. part 310, DoD Privacy Program, 32 C.F.R. part 311, Office of the Secretary of Defense and Joint Staff Privacy Program, and DoD 5400.11-R, Department of Defense Privacy Program, and Executive Order 9397, as amended.

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 purpose of PAWS is to process Privacy Act (PA) requests and administrative appeals in accordance with the Privacy Act of 1974. Individuals submitting Privacy Act requests to the DoD CAF provide their Personally Identifiable Information (PII) in order for the DoD CAF Privacy Act Office to verify identity and retrieve responsive records from available systems of record. The requests generally contain a person's full name(s), social security number (SSN), Address(es), Phone Number (optional), E-mail Address (optional), Data and Place of Birth, and Attorney or representative name/contact information, and a brief description of requested records.

Other types of information the system contains include personal, medical, and financial information pertaining to the individual.

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

Risks include, but are not limited to, identity theft, loss of employment, unwarranted public revelation of private data, targeting, etc.

To mitigate risk, access to records is role base and one must have user name/password to gain access. The only users authorized access to the system are DoD CAF Privacy Office staff and IT professionals. To prevent unwarranted disclosure of personal information, system users are provided initial and follow-up training to comply with established privacy and security policies and procedures. In addition, the building is protected by alarm systems, and armed guards, 24 x 7 access control measures. Hardcopy documents are maintained in a locked container when not in use.

The use of manual and automated redaction, along with security based attribute/special markings at the user and object level, safeguards PII data.

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.

Under the Privacy Act, an individual initiates the request for records pertaining to themselves. It is necessary for the requester to provide specific personally identifiable information in order for the DoD CAF Privacy Act Office to verify the identity of the person, conduct an adequate search of responsive records, and retrieve available records. Providing the information is voluntary; however, without it the DoD CAF will not be able to process their request.

(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.

Individuals may consent to the release of their personal information to a third-party or legal representative.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The following Privacy Act Statement is provided on the DoD CAF Form 3, Request for Records.

Authorities: 5 U.S.C. 552a, the Privacy Act of 1974, as amended; 10 U.S.C. 113, Secretary of Defense; 32 CFR part 310 DoD Privacy Program; 32 CFR part 311, OSD Privacy Program; DoD 5400.11-R, Department of Defense Privacy Program; and E.O. 9397 (SSN), as amended. Principal Purpose(s): To ensure needed information is collected so that your request for access to the records about you maintained by the DoD Consolidated Adjudications Facility can be processed. These records will also be used in any Privacy Act appeals or related litigation. These records are covered by DWHS E04, Privacy Act Case Files found at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570753/dwhs-e04.aspx>. Routine Use(s): The Law Enforcement, Congressional Inquiries, Department of Justice for Litigation, National Archives and Records Administration, and Data Breach Remediation, and Routine Uses found at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> may apply. Disclosure: Voluntary. However, if the information needed to locate your records and send your response is not provided, we will not be able to respond to your request. The Social Security Number is used to retrieve adjudication files.

Additionally, a Privacy Advisory is given to the requester when we request additional PII data elements in order to perfect a request. The requester is notified that the information is necessary to conduct an adequate search of responsive records.

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.