



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Sexual Assault Advocate Certification Program

Defense Human Resources Activity

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.

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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; DTM 14-001, Defense Sexual Assault Advocate Certification Program (D-SAACP).

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.

To track the certification of Sexual Assault Response Coordinators (SARC) and Sexual Assault Prevention and Response Victim Advocates (SAPR VA). Information will be used to process applications, and review and report on the status of SARC and SAPR VA certification to Congress.

The system will includes: Applicant's first name, middle initial, and last name; position type (Sexual Assault Response Coordinator (SARC) or Sexual Assault Prevention Representative Victim Advocate (SAPR VA)); Service/DoD affiliation and status; grade/rank; installation/command; work email address and telephone number; official military address of applicant and applicant's SARC (commanding officer, street, city, state, ZIP code, country); position level (Level I, II, III, or IV); certificates of training; date of application; verification of sexual assault victim advocacy experience (position, dates, hours, supervisor; name, title, and work telephone number of verifier); evaluation of sexual assault victim experience (description of applicant skills, abilities, and experience; name, title, and office of evaluator), letters of recommendation by the first person in the chain of command, SARC, and the Senior Commander or the Commander; supervisor and commander statement of understanding, documentation of continuing education training courses; Defense Sexual Assault Advocate Certification Program (D-SAACP) identification (ID) number.

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

The privacy risk associated with this collection of PII include unauthorized access by employees who do not have a need to access the data and unauthorized disclosure of the information.

D-SAACP will collect data, in a manner consistent with DoD privacy regulations, on those DoD military and civilian personnel applying for Certification as a SARC or SAPR VA. Records are maintained in a controlled facility that employs physical restrictions such as double locks and is accessible only to authorized persons who hold key fobs. Access to electronic data files in the system is role-based, restricted to essential personnel only, and requires the use of a password. The data server is locked in a windowless room with restricted access. Data is encrypted, and backup data is also encrypted and removed to an off-site secure location for storage. Paper files are stored in a locked filing cabinet in a locked room in the controlled facility. System access to case files will be limited to computers within a closed network, not connected to the internet or other servers.

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.

SARCs and SAPR VAs may object to the collection of their PII by not submitting their PII on the required forms. However, they may not be considered qualified to perform their duties as a SARC and SAPR VA if they do not submit the information required to become certified.

(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.

Applicants cannot give or withhold their consent to specific uses of their PII. The PII will be used in very limited ways, including to process and grant certification and communicate to the applicants and the DoD on certification status.

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.

DD Form 2950, Department of Defense Sexual Assault Advocate Certification Program New Application Packet and DD Form 2950-1, Department of Defense Sexual Assault Advocate Certification Program Renewal Application Packet, includes a Privacy Act Statement on the first page as follows:

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 6495.01; DoD Instruction 6495.02; DTM 14-001.

PRINCIPAL PURPOSE(S): The information provided on this form will be used to review and process applications for Sexual Assault Response Coordinator (SARC) and Sexual Assault Prevention Representative (SAPR) Victim Advocate (VA) certification.

ROUTINE USE(S): The DoD "Blanket Routine Uses" at <http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> may apply.

DISCLOSURE: Voluntary. However, if you are a SARC or SAPR VA and do not complete this form to become certified, you may be disqualified from the position. 10 U.S.C. 1561, note requires DoD to establish a certification program.

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.