



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Victim-Related Inquiry Tracking Files

Sexual Assault Prevention and Response Office (SAPRO)

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

DHRA xx

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.

TBD

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

TBD

Enter Expiration Date

TBD

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. 1561 note, Improved Sexual Assault Prevention and Response in the Armed Forces; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

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 victim-related inquiries (VRI) received by the Sexual Assault Prevention and Response Office (SAPRO) via e-mail, SAPRO.mil, the DoD Safe Helpline, phone, or mail. Once received, inquiries are referred to the appropriate agency POC and/or to the DoD IG for any complaints concerning the Military Criminal Investigative Organization in order to address the issue(s) raised and facilitate a resolution.

SAPRO collects the following, where applicable: inquirer's name, telephone number, email address, home address, relationship to the victim, and victim inquiry number; how the inquiry was received (written, email, telephone), type of inquiry (e.g. Army, Navy, Air Force, legal, command, law enforcement, inspector general, medical, Safe Helpline, report of sexual assault, training, etc.), and category of inquiry (e.g. general complaint, criticism of SAPR Personnel program, general information request, raising a policy issue, report of misconduct, request for Service referral, report of retaliation, praise of SAPR personnel or program); victim's name, Service affiliation, status/position, and installation; date of incident, year assault was reported, if command and/or a Military Criminal Investigation Office was involved, and case synopsis; name and title of office or official about which the inquirer is commenting; documents that inquirer submits to SAPRO; permission for SAPRO to follow up on the inquiry; agency to which the inquiry was referred, agency action officer name, documents sent to or received from relevant agency in support of the inquiry, suspense date, and case synopsis sent to the agency; dates that final status was sent to requester and date the inquiry was closed; comments and dates tracking communication between SAPRO, agencies, and inquirer. This information may be provided by utilizing the DD Form 2985.

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

If improperly disclosed or breached, there is a risk that the PII in VRI could identify individuals as a victim of a sexual assault involving a member of the Armed Forces.

In order to safeguard individual privacy, SAPRO ensures data is collected and maintained in a manner consistent with DoD policy and regulations related to privacy, as well as the reporting of sexual assaults involving a member of the Armed Forces. Additionally, records are maintained in a controlled facility that employs physical safeguards including the use of combination locks and identification badges. Access to electronic data files in the system is role-based, restricted to personnel with a need to know, and requires a Common Access Card (CAC) and password. Electronic data is also protected via encryption. The database cannot be accessed from the outside as it does not reside on a server and all records are accessible only to authorized persons with a need to know who are properly screened, cleared, and trained.

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.

DoD Inspector General; DoD Family Advocacy Program, Army, Navy, Marine Corps, National Guard

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.

Voluntary; however, failure to provide information may limit SAPRO's ability to provide requested assistance.

(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.

The individual must provide consent to have their PII and complaint forwarded to the appropriate agency for action and/or assistance.

(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.

Authority: 10 U.S.C. 1561 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 47, Uniform Code of Military Justice; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

Principle Purposes: To track victim-related inquiries received by the Sexual Assault Prevention and Response Office (SAPRO) via email, SAPRO.mil, the DoD Safe Helpline, phone, or postal service. Once received, inquiries are referred to the appropriate agency POC and/or to the DoD IG in order to address the issue(s) raised and facilitate a resolution.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Congressional Inquiries Disclosure Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at: <http://dpclid.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>

Disclosure: The completion of this form is voluntary. However, failure to provide information may result in the inability to provide requested services.

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.