PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Sexual Assault Incident Database (DSAID)
Office of the Under Secretary of Defense (OUSD) for Personnel and Readiness (P&R)

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: 11499
- ☐ **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 007-97-01-20-02-3659-00

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 06

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. Pending submission

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. 113 note; 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; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 600-20, Sexual Assault Prevention and Response (SAPR) Program; 10 U.S. C. 5013, Secretary of the Navy; Secretary of the Navy Instruction 1752.4A, Sexual Assault Prevention and Response; Marine Corps Order 1752.5A, Sexual Assault Prevention and Response (SAPR) Program; 10 U.S.C. 8013, Secretary of the Air Force; Air Force Instruction 36-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397, as amended (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.

To centralize case-level sexual assault data involving a member of the Armed Forces, including information, if available, about the nature of the assault, the victim, the alleged perpetrator, and case outcomes in connection with the assault. At the local level, Sexual Assault Response Coordinators and Victim Advocates work with victims to ensure that they are aware of services available, and that they have contact with medical treatment personnel and DoD law enforcement entities. At the DoD level, only de-identified data is used to respond to mandated reporting requirements. The DoD Sexual Assault Prevention and Response Office has access to identified closed case information and de-identified, aggregate open case information for study, research, and analysis purposes.

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

The Defense Sexual Assault Incident Database (DSAID) collects victim and alleged perpetrator personal identifiers, incident information, and case outcomes in connection with the assault. In order to safeguard individual privacy, records are maintained in a controlled facility. Physical entry is restricted by the use of alarms, cipher and 509 locks, armed guards, and slow access. Access to case files in the system is role-based and requires the use of a Common Access Card and password. Further, at the DoD-level, only de-identified data can be accessed.

DSAID will reside on the Washington Headquarters Services network. The protections on the network will include firewalls, passwords, and web-common security architecture. In addition, the local drive will reside behind the firewall on the safe side; the direct database cannot be accessed from the outside; and the system rests on the Nonsecure Internet Protocol Router Network.

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. Office of the Secretary of Defense

☒ **Other DoD Components.**

Specify. Army, Marine Corps, Navy, Air Force and the National Guard Bureau

☐ **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.

DSAID will collect information regarding Military personnel, DoD civilians, or contractors who may be victims and/or alleged perpetrators in a sexual assault involving a member of the Armed Forces.

Sexual Assault Response Coordinators will read victims the Privacy Act Statement. Alleged perpetrator PII data are collected by Service Military Criminal Investigative Organizations and Offices of the Judge Advocate General systems and are loaded into DSAID after reasonable suspicion has been found that the alleged perpetrator may have committed the crime.

(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.

Victims of sexual assault have two options when reporting information regarding an incident. Individuals may consent to a full collection of information, which will initiate legal proceedings, or they may report in a way that enables them to receive assistance without legal obligation. If necessary information is withheld at the time the incident is reported, the case may not be able to proceed or be closed.

Alleged perpetrator PII data are collected by Service Military Criminal Investigative Organizations and Office of the Judge Advocate Generals systems and are loaded into DSAID after reasonable suspicion has been found that the alleged perpetrator may have committed the crime.

(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.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.	Sexual Assault Response Coordinators will read victims the Privacy Act Statement.

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.