PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Sexual Assault Incident Database (DSAID)
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**
- ☐ **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 007-97-01-03-02-3659-00

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

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 0704-0482

Enter Expiration Date 09/30/2015

☐ **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; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 32 U.S.C. 102, National Guard; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; Army Regulation 600-20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); Secretary of the Navy Instruction 1752.4B, Sexual Assault Prevention and Response; Marine Corps Order 1752.5B, Sexual Assault Prevention and Response (SAPR) Program; Air Force Instruction 90-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), 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.

To centralize case-level sexual assault data involving a member of the Armed Forces, in a manner consistent with statute and DoD regulations for Unrestricted and Restricted reporting. Records include information, if available, about the nature of the assault (e.g., incident date and location, type of offense), victim, alleged perpetrator, investigation, case outcomes in connection with the assault, and other information necessary to fulfill reporting requirements.

Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, conducting research, and case and business management. De-identified data may also be used to respond to mandated reporting requirements.

Victim and alleged perpetrator information includes: Age at the time of incident; gender, race, ethnicity; affiliation (e.g., military, DoD civilian/contractor, other government employee, U.S. civilian, foreign national/ military, unknown, and military dependent); Service, grade/rank, status (e.g., Active Duty, Reserve, National Guard); and location of assignment and incident. Additional victim and alleged peretrator information, maintained in Unrestricted Reports only, includes: full name; identification type and number (e.g., DoD Identification number, Social Security Number, passport, U.S. Permanent Residence Card, foreign identification); and date of birth.

Additional victim information includes: Defense Sexual Assault Incident Database (DSAID) control number (i.e., system generated unique control number) and relationship to alleged perpetrator. Additional victim information, maintained in Unrestricted Reports only includes: work or personal contact information (e.g., phone number, address, email address); and name of commander.

For Restricted Reports (reports that do not initiate investigation), no personally identifying information for the victim and/or alleged perpetrator is maintained in DSAID.

Other data collected to support case and business managementincludes: date and type of report (e.g., Unrestricted or Restricted); tracking information on Sexual Assault Forensic Examinations performed, and referrals to appropriate resources; information on line of duty determinations; victim safety information; case management meeting information; and information on memoranda of understanding. For Unrestricted reports, information on expedited transfers and civilian/military protective orders may also be collected.

(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 DSAID could identify individuals as either a victim or alleged perpetrator of a sexual assault involving a member of the Armed Forces.

In order to safeguard individual privacy, records are maintained in a controlled facility. Physical entry is restricted by the use of guards, identification badges, key cards, and locks. Access to case files in the system is role-based and requires the use of a Common Access Card (CAC) and password. Access rights and permission lists for Sexual Assault Response Coordinators (SARCs) and authorized Military Service legal officers are granted by Military Service Sexual Assault Prevention and Response program managers or by the SAPRO DSAID Program Manager through the assignment of appropriate user roles. Periodic security audits are also conducted. Technical safeguards include firewalls, passwords, encryption of data, and use of a virtual private network. In addition, the local drive resides behind a firewall and the direct database cannot be accessed from the outside.

DSAID further collects and maintains all data in a manner consistent with DoD policy and regulations for Unrestricted and Restricted Reporting.

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. SAPR Program Managers, Sexual Assault Response Coordinators, and authorized Legal Officers (i.e. attorneys provided access to the system) of the Army, Navy, Marine Corps, Air Force, and National Guard Bureau

☒ **Other Federal Agencies.**

Specify. Department of Veterans Affairs

☐ **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.

Victims are asked for their information by Sexual Assault Response Coordinators. When reporting information regarding an incident victims have two options, Restricted or Unrestricted reporting. If a victim of a sexual assault involving a member of the Armed Forces makes a Restricted Report of sexual assault, no personally identifying information for the victim is collected or maintained.

(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 are asked for their information by Sexual Assault Response Coordinators. When reporting information regarding an incident victims have two options, Restricted or Unrestricted reporting.

Restricted reporting allows sexual assault victims to confidentially disclose the assault to specified individuals (i.e., SARC, SAPR Victim Advocate (VA), or healthcare personnel) and receive medical treatment, including emergency care, counseling, and assignment of a SARC and SAPR VA, without triggering an official investigation. The victim's report provided to healthcare personnel (including the information acquired from a Sexual Assault Forensic Examination Kit), SARCs, or SAPR VAs are not reported to law enforcement or to the command to initiate an official investigative unless the victim consents or an established exception applies in accordance with DoD Instruction 6495.02, "Sexual Assault Prevention and Response (SAPR) Program Procedures."

Unrestricted reporting allows a victim to disclose, without requesting confidentiality or Restricted Reporting, that he or she is the victim of a sexual assault. Under these circumstances, the victim's report provided to healthcare personnel, the SARC, a SAPR VA, command authorities, or other persons is reported to law enforcement and may be used to initiate an official investigative process.

(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.

SARCs read victims the Privacy Act Statement when they elect to report on the DD Form 2910, "Victim Reporting Preference Statement," which states the following:

AUTHORITY: 10 U.S.C. 113 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 136; 32 U.S.C.; DoD Directive 6495.01; DoD Instruction 6495.02; 10 U.S.C. 3013; Army Regulation 600-20, Chapter 8; 10 U.S.C. 5013; Secretary of the Navy Instruction 1752.4A; Marine Corps Order 1752.5A; 10 U.S. C. 8013; Air Force Instruction 36-6001; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): Information will be used to document elements of the sexual assault response and/or reporting process and comply with the procedures set up to effectively manage the sexual assault prevention and response program. At the local level, Service SAPR Program Management, Major Command Sexual Assault Response Coordinator(s) (SARCs), Installation and

Brigade SARCs use information to ensure that victims are aware of services available and 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 congressional 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 congressional reporting, study, research, and analysis purposes. Collected information is covered by DHRA 06 DoD, Defense Sexual Assault Incident Database (http://dpclo.defense.gov/Privacy/SORNsIndex/tabid/5915/Article/6841/dhra-06-dod.aspx).

ROUTINE USE(S): The DoD blanket routine uses found at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx may apply to this record. Note: Any release made as a blanket routine use will be consistent with the principal purpose of its original collection.

DISCLOSURE: Voluntary. However, if you decide not to provide certain information, it may impede the ability of the SARC to offer the full range of care and support established by the Sexual Assault Prevention and Response program. You will not be denied advocacy services or healthcare (medical and mental health) because you selected the Restricted Reporting option. The Social Security Number (SSN) is one of several unique personal identifiers that may be provided. This form will be retained for 50 years.

DD2965, "Defense Sexual Assault Incident Database (DSAID) Data Form" also states:

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 32 U.S.C. 102, National Guard; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; Army Regulation 600-20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); Secretary of the Navy Instruction 1752.4B, Sexual Assault Prevention and Response; Marine Corps Order 1752.5B, Sexual Assault Prevention and Response (SAPR) Program; Air Force Instruction 90-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): The information collected documents elements of the sexual assault response and/or reporting process and will be entered into the Defense Sexual Assault Incident Database to comply with the procedures set up to effectively manage the sexual assault prevention and response program. At the local level, Service SAPR Program Management, Major Command Sexual Assault Response Coordinator(s) (SARCs) and Installation SARC(s) use this information to ensure that victims are aware of services available and 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 congressional 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 congressional reporting, study, research, and analysis purposes. The applicable Privacy Act System of Records Notice is DHRA 06, Defense Sexual Assault Incident Database found at http://dpcld.defense.gov/privacy/SORNs/component/osd/DHRA06DoD.html

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.
To permit the disclosure of records of closed cases of unrestricted reports to the Department of Veterans Affairs (DVA) for purpose of providing medical care to former Service members and retirees, to determine the eligibility for or entitlement to benefits, and to facilitate collaborative research activities between the DoD and DVA.
Applicable Blanket Routine Use(s) are: (1) Law Enforcement Routine Use, (2) Disclosure When Requesting Information Routine Use, (3) Disclosure of Requested Information Routine Use, (4) Congressional Inquiries, (8) Disclosure to the Office Personnel Management Routine Use, (9) Disclosure to the Department of Justice for Litigation Routine Use, (12) Disclosure of Information to the National Archives and Records Administration Routine Use, (13) Disclosure to the Merit systems Protection Board Routine Use, and (15) 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://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

DISCLOSURE: Voluntary. However, if you decide not to provide certain information, it may impede the ability of the SARC to offer the full range or care and support established by the sexual assault prevention and response program. You will not be denied benefits via the Restricted Reporting option. For Unrestricted Reports, the Social Security Number (SSN) is one of several unique personal identifiers that may be provided. Some alternatives include state driver's license number, passport number, or DoD ID number.

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.