PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Sexual Assault Incident Database (DSAID)

2. DOD COMPONENT NAME:

Department of Defense Human Resources Activity

3. PIA APPROVAL DATE:

Sexual Assault Prevention and Response Office (SAPRO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☒ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and 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. To facilitate reports to Congress on claims of retaliation in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Forces. To facilitate Unrestricted Reports to Congress on the adult sexual assault cases reported by the Family Advocacy Program (FAP).

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

The DSAID File Locker Module is also used to maintain Victim Reporting Preference Statements and DoD Sexual Assault Forensic Examination (SAFE) Reports in a secure, encrypted environment, in accordance with appropriate records retention schedules.
Victim and alleged perpetrator information includes: Age at the time of incident; sex, 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); occupation, location of assignment and incident. Additional victim and alleged perpetrator information, maintained in Unrestricted Reports only, includes: Full name; identification type and number (e.g., DoD Identification number (DoD ID); passport; U.S. Permanent Residence Card; foreign identification; Social Security Number (SSN) to allow for DoD law enforcement entities to update the record with investigatory information); date of birth; and case disposition information;

Additional victim information includes: 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.

Restricted Reports (reports that do not initiate investigation), may contain personally identifiable information from the Victim Reporting Preference Statement or other sources for the victim and/or alleged perpetrator; no information on reports of retaliation is maintained.
Other sexual assault data collected to support case and business management includes: Date and type of report (e.g., Unrestricted or Restricted); tracking information on SAFEs 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.
Retaliation reporter and alleged retaliator information includes: Full name; DoD ID; date of birth; sex, race, ethnicity; affiliation (e.g., military, DoD civilian/contractor, other government employee, and military dependent); duty status, pay grade; location of assignment; and case disposition information.
Additional retaliation reporter information includes: Other identification type and number (e.g., passport; U.S. Permanent Residence Card;

foreign identification; SSN to allow for DoD law enforcement entities to update the record with investigatory information); retaliation control number (i.e., system generated unique control number).
Other retaliation data collected to support case and business management includes: DSAID control number, tracking information on actions taken to support reporter of retaliation; nature and findings of the retaliation investigation; relationship between alleged retaliator and retaliation reporter; relationship between alleged retaliator and alleged perpetrator of sexual assault; and phone number.
Records maintained for the DSAID File Locker include: Victim Reporting Preference Statement (includes victim full name, SSN, and DoD ID number), Unrestricted Reports are maintained in a searchable format, whereas Restricted Reports are maintained in a non-searchable format and can only be accessed with an encryption key; SAFE; year and month of report, SARC's assigned location, installation name, DSAID control number, and/or SARC affiliation may be maintained as metadata. Last four of the SSN, date of birth, mother's maiden name, and state or country of birth may also be maintained for use as an encryption key to grant access for victims and retaliation reporters to their Restricted Report records. military, DoD civilian/contractor, other government employee, and military dependent); duty status, pay grade; location of assignment; and case disposition information.

Additional retaliation reporter information includes: Other identification type and number (e.g., passport; U.S. Permanent Residence Card; foreign identification; SSN to allow for DoD law enforcement entities to update the record with investigatory information); retaliation control number (i.e., system generated unique control number).

Other retaliation data collected to support case and business management includes: DSAID control number, tracking information on actions taken to support reporter of retaliation; nature and findings of the retaliation investigation; relationship between alleged retaliator and retaliation reporter; relationship between alleged retaliator and alleged perpetrator of sexual assault; and phone number.

Records maintained for the DSAID File Locker include: Victim Reporting Preference Statement (includes victim full name, SSN, and DoD ID number), Unrestricted Reports are maintained in a searchable format, whereas Restricted Reports are maintained in a non-searchable format and can only be accessed with an encryption key; SAFE; year and month of report, SARC's assigned location, installation name, DSAID control number, and/or SARC affiliation may be maintained as metadata. Last four of the SSN, date of birth, mother's maiden name, and state or country of birth may also be maintained for use as an encryption key to grant access for victims and retaliation reporters to their Restricted Report records military, DoD civilian/contractor, other government employee, and military dependent); duty status, pay grade; location of assignment; and case disposition information.

Additional retaliation reporter information includes: Other identification type and number (e.g., passport; U.S. Permanent Residence Card; foreign identification; SSN to allow for DoD law enforcement entities to update the record with investigatory information); retaliation control number (i.e., system generated unique control number).

Other retaliation data collected to support case and business management includes: DSAID control number, tracking information on actions taken to support reporter of retaliation; nature and findings of the retaliation investigation; relationship between alleged retaliator and retaliation reporter; relationship between alleged retaliator and alleged perpetrator of sexual assault; and phone number.

Records maintained for the DSAID File Locker include: Victim Reporting Preference Statement (includes victim full name, SSN, and DoD ID number), Unrestricted Reports are maintained in a searchable format, whereas Restricted Reports are maintained in a non-searchable format and can only be accessed with an encryption key; SAFE; year and month of report, SARC's assigned location, installation name, DSAID control number, and/or SARC affiliation may be maintained as metadata. Last four of the SSN, date of birth, mother's maiden name, and state or country of birth

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Identification and Verification

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Sexual assault victims are asked for their information by Sexual Assault Response Coordinators (SARCs) and must sign a DD2910, "Victim Reporting Preference Statement" to initiate an official report. When reporting information regarding a sexual assault 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.

Reports of retaliation may only be made in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Force. Retaliation reporters must sign DD Form 2910-2, "Retaliation Reporting Statement for Unrestricted Sexual Assault Cases" to initiate an official report.

f. 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.

Sexual assault victims are asked for their information by SARCs and can elect one of two reporting options, Restricted or Unrestricted.

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.

Reports of retaliation may only be made in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Forces. Retaliation reporters, however, do not have the option to confidentially disclose the retaliation. All official reports of retaliation will be maintained in DSAID and include the reporters' PII

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

DD Form 2910, "Victim Reporting Preference Statement"
AUTHORITY: 110 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 7013, Secretary of Army, 10 U.S.C. 8013, Secretary of the Navy, 10 U.S.C. 9013, Secretary of the Air Force, 10 U.S.C. 9081, United States Space Force, 32 U.S.C. 102, National Guard; DoD Directive 6495.01, (Sexual Assault Prevention and Response Program); Army Regulation 600-20 (Army Command Policy) Chapter 8, Office of the Chief of Naval Operations (OPNAV) Instruction 1752.1C, Sexual Assault Prevention and Response Program; Marine Corps Order 1752.5C, SAPR Program, Air Force Instruction 90-6001, SAPR Program, 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 procedures set up to effectively manage the Sexual Assault Prevention and Response Program.

ROUTINE USE(S): Applicable Routine Use(s) are: To Permit the disclosure of records of closed cases of unrestricted reports to the Department of Veterans Affairs (DVA) for purpose of providing mental and medical care to former Service members, to determine the eligibility for or entitlement to benefits, and to facilitate collaborative research activities between the DoD and DVA. Additional routine uses are listed in the applicable system of records notice, DHRA 06, Defense Sexual Assault Incident Database (DSAID), at https://dpcid.defense.gov/Privacy/SORNsinex/DOD-wide-SORN-Article-View/Article/570559/dhra-06-dod/.
DD Form 2910-1, REPLACEMENT OF LOST DD Form 2910, VICTIM REPORTING PREFERENCE STATEMENT

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 8013, Secretary of the Navy; 10 U.S.C. 9013, Secretary of the Air Force; 10 U.S.C. 9081, United States Space Force; 32 U.S.C. 102, National Guard; DoD Directive 6495.01, (Sexual Assault Prevention and Response Program); Office of the Chief of Naval Operations (OPNAV) Instruction 1752.1C, Sexual Assault Prevention and Response Program; Marine Corps Order 1752.5C, SAPR Program; Air Force Instruction 90-6001, SAPR Program, 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 (SAPR) Program. Specifically, the form will document the loss of the original DD Form 2910 through the request for a replacement form. The form shall document the reaffirmation or change of the original reporting option. At the local level, Service SAPR Program Management, Major Command Sexual Assault Response Coordinator(s) (SARCs), Installation, and Brigade SARCs use the 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.

ROUTINE USE(S): The DoD blanket routine uses found at http://dcpio.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 the information's

original collection. Collected information is covered by Department of Human Resources Activity 06 DoD, Defense Sexual Assault Incident Database (https://dpcid.defense.gov/Privacy/SORNsinex/DOD-wide-SORN-Article-View/Article/570559/dhra-06-dod/).

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.
DD2910-2, "Retaliation Reporting Statement for Unrestricted Sexual Assault Cases"

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 7013, Secretary of Army, 10 U.S.C. 8013, Secretary of the Navy, 10 U.S.C. 9013, Secretary of the Air Force, 10 U.S.C. 9081, United States Space Force, 32 U.S.C. 102, National Guard; DoD Directive 6495.01, (Sexual Assault Prevention and Response Program); Army Regulation 600-20 (Army Command Policy) Chapter 8, Office of the Chief of Naval Operations (OPNAV) Instruction 1752.1C, Sexual Assault Prevention and Response Program; Marine Corps Order 1752.5C, SAPR Program, Air Force Instruction 90-6001, SAPR Program, and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): Information will be used to document reports of retaliation and elements of the response related to retaliation reports when the retaliation is associated with an Unrestricted Report of sexual assault. SAPR Program personnel use information to ensure that victims are aware of available services. At the DoD level, only de-identified data is used to respond to mandated congressional reporting requirements.

ROUTINE USE(S): Applicable Routine Use(s) are: To Permit the disclosure of records of closed cases of unrestricted reports to the Department of Veterans Affairs (DVA) for purpose of providing mental and medical care to former Service members, to determine the eligibility for or entitlement to benefits, and to facilitate collaborative research activities between the DoD and DVA. Additional routine uses are listed in the applicable system of records notice, DHRA 06, Defense Sexual Assault Incident Database (DSAID), at https://dpcid.defense.gov/Privacy/SORNsinex/DOD-wide-SORNArticle-View/Article/570559/dhra-06-dod/

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"

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 7013, Secretary of Army, 10 U.S.C. 8013, Secretary of the Navy, 10 U.S.C. 9013, Secretary of the Air Force, 10 U.S.C. 9081, United States Space Force, 32 U.S.C. 102, National Guard; DoD Directive 6495.01, (Sexual Assault Prevention and Response Program); Army Regulation 600-20 (Army Command Policy) Chapter 8, Office of the Chief of Naval Operations (OPNAV) Instruction 1752.1C, Sexual Assault Prevention and Response Program; Marine Corps Order 1752.5C, SAPR Program, Air Force Instruction 90-6001, SAPR Program, and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): 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. To facilitate reports to Congress on claims of retaliation in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Forces. 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. The DSAID File Locker, a separate module within the system, is used to maintain Victim Reporting Preference Statements and DoD Sexual Assault Forensic Examinations (SAFEs) to ensure compliance with federal records retention requirements and allow victims and reporters to access these forms for potential use in Department of Veterans Affairs (DVA) benefits applications.
https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DHRA-06-DoD.pdf

ROUTINE USE(S): Information provided may be further disclosed to the Department of Veteran's Affairs for benefits purposes and to facilitate collaborative research activities between the DoD and DVA. In addition, this form is subject to the proper and necessary routine uses identified in the system of records notice(s) specified in the purpose statement above. In addition to those disclosures generally permitted in accordance with 5 U.S.C. 552a(b), the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☐ Within the DoD Component	Specify.	
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*		SAPR Program Managers, Sexual Assault Response

Specify. Coordinators, and authorized Legal Officers (i.e. attorneys provided access to the system) of the Army, Navy, Marine Corps, Air Force, Space Force, National Guard Bureau; DoD, and Office of the Inspector General

☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*

Specify. Department of Veterans Affairs, Coast Guard, Government Accountability Office (GAO)

☐ State and Local Agencies

Specify.

☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*

Specify.

☐ Other *(e.g., commercial providers, colleges).*

Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☐ Databases
☒ Existing DoD Information Systems
☐ Commercial Systems
☐ Other Federal Information Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☒ E-mail
☒ Official Form (*Enter Form Number(s) in the box below)*
☒ In-Person Contact
☐ Paper
☐ Fax
☒ Telephone Interview
☒ Information Sharing - System to System
☐ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

DD Form 2910; DD Form 2965; DD 2910-1; DD Form 2910-2; DD Form 2910-3; DD Form 2910-4; DD Form 2910-5; DD Form 2910-6; DD Form 2910-7, DD Form 2910-8

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DHRA 06

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-0330-2013-0005

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cutoff cases at the end of the fiscal year and destroy 50 years after cutoff.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 932, Art. 132 Retaliation; 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; 10 U.S.C. 9081, United States Space Force; 32 U.S.C. 102, National Guard; DoD Directive 6495.01, SAPR Program; DoD Instruction 6495.02, SAPR Program Procedures; Army Regulation 600–20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); OPNAV Instruction 1752.1C, SAPR Program; Marine Corps Order 1752.5C, SAPR Program; Air Force Instruction 90–6001, SAPR Program; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0482, Defense Sexual Assault Incident Database, Expiration Date: 03/31/2025
(https://omb.report/search.php?terms=0704-0482)