

SYSTEM NAME AND NUMBER: DoD Sexual Assault Prevention and Response Office Victim Assistance Data Systems, DHRA 18 DoD. (October 12, 2018; 83 FR 51675)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: DoD Sexual Assault Prevention and Response Office (SAPRO), 4800 Mark Center Drive, Alexandria, VA 22350-1500. Amazon Web Services (AWS), 12900 Worldgate Drive, Suite 800, Herndon, VA 20170-6040.

SYSTEM MANAGER(S): Senior Victim Assistance Advisor, DoD SAPRO, 4800 Mark Center Drive, Alexandria, VA 22350-1500; telephone 571-372-2657; email whs.mc-alex.wso.mbx.SAPRO@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 28 CFR 115, Prison Rape Elimination Act National Standards; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

PURPOSE(S) OF THE SYSTEM: To track victim-related inquiries and follow-up support service requests by the SAPRO via email, SAPR.mil, the DoD Safe Helpline (SHL), phone, or mail; to respond to requests for SHL marketing and promotional materials; to allow individuals to provide feedback on the services of a sexual assault response coordinator (SARC), victim advocate, or other military staff or employee on their installation/base; to maintain a searchable referrals database that houses contact information for SARCs, medical, legal, chaplain, military police resources, and civilian sexual assault service providers; to provide user access to the Safe Helpline Report Database; to track and facilitate unrestricted and anonymous notifications of sexual abuse and harassment in Military Correctional Facilities, in accordance with the Prison Rape Elimination Act (PREA).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who request materials or provide feedback on military sexual assault services; SARCs, medical, legal, chaplain, military police, and civilian sexual assault responders; Reportable database users; and individuals who contact the DoD SHL or SAPRO for assistance, follow-up support services, or who provide information about sexual abuse and harassment occurring at Military Correctional Facilities under the Prison Rape Elimination Act.

CATEGORIES OF RECORDS IN THE SYSTEM: For inquiries, feedback, or support requests the following information may be collected: Requestor/inquirer's full name or pseudonym, personal/work telephone number and email address, home address, user type/position (e.g. victim/survivor, family friend, Service member, military spouse, DoD civilian employee, etc.), Service affiliation, rank, base/installation, state, and age; how the inquiry was received (written, email, telephone), type of inquiry (e.g., Army, Navy, Air Force, legal, command, law enforcement, inspector general, medical, DoD Safe Helpline, report of sexual assault, training, etc.), and category of inquiry (e.g., general complaint, criticism of SAPR Personnel or 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, installation, and inquiry number; installation where the

interaction took place, date of incident, the name and/or office and title of the military personnel about which the feedback is being submitted, year assault was reported, if command and/or a Military Criminal Investigation Office was involved, and case synopsis; 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.

PREA notifications may include: Type of notification (e.g., anonymous report via SAPRO, Unrestricted report via SARC, Unrestricted report via SAPRO, etc.); date and time of notification; location and date/time of the incident; victim's full name (for unrestricted reports); caller's full name (for unrestricted reports); caller's contact information (as applicable); caller's relationship to the victim (self or third party); permission from inmate for SAPRO to forward the notification for investigation; SARC location and phone number (unrestricted reports only) and details provided by the caller about the nature of the incident (not including PII for all anonymous reports).

When requesting materials about the Program, the following information may be collected: First and last name, shipping address, personal or work email, installation/base, rank (if applicable), status/position (e.g., Sexual Assault Response Coordinator (SARC), victim advocate, third party organization, etc.), affiliation (e.g., Service, family member, veteran, etc.), and an open comment field for questions and suggestions.

For the DoD and civilian responders the following information may be collected: Name and work-related contact information (installation/base, address, email, phone number).

RECORD SOURCE CATEGORIES: The individual.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, 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:

- a. To the Department of Veterans Affairs to facilitate the resolution of questions regarding benefits and care in support of a diagnosis with the Veterans Health Affairs related to Military Sexual Trauma and with the Veterans Benefits Affairs in obtaining benefits.
- b. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
- c. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction

with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

- d. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
- e. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- f. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
- g. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- h. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed there was a breach of the system of records; (2) the DoD determined as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- i. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: System records are stored on electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Name; date of inquiry; and/or Military Correctional Facility, as appropriate.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
Victim Related-Inquiry Tracking Files (DD Form 2985 and 2985-1): Records are destroyed 25 years after the end of the calendar year in which the case was resolved.

DD Form 2985-2, Materials Request: Records are destroyed three (3) months after the end of the fiscal year in which the request for material was completed or cancelled.

Responder Database: Obsolete and revised are destroyed one (1) year after the end of the fiscal year.

Reportal Administrative Database: After three (3) continuous years of inactivity, records are closed at the end of that fiscal year; and destroyed after an additional 25 years.

Follow-up Support System: Records are destroyed 25 years after the end of the fiscal year of the close-out of the communication.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Victim-related inquiry records are maintained in a controlled facility employing 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.

SHL servers are maintained within the Amazon Web Services (AWS) GovCloud network infrastructure. The protections on the network include firewalls, passwords, and web-common security architecture. AWS restricts physical access to the data centers where the SHL servers reside. Physical access logs are reviewed and analyzed on a daily basis by AWS personnel. All PII is stored in a password-protected environment with internal access only. All individuals with access to the data undergo a background investigation and sign a nondisclosure agreement.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed, written requests should contain the name of the individual, the name and number of this system of records notice, date of incident and/or Military Correctional Facility, if applicable.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: The OSD rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to Senior Victim Assistance Advisor, DoD SAPRO, Victim Assistance, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

Signed, written requests should contain the name of the requester, the name of the original inquirer, the name of the victim, date of incident and/or Military Correctional Facility, if applicable.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: N/A.