DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on an Altered System of Records
Under the Privacy Act of 1974

1. System identifier and name: DHRA 06, entitled "Defense Sexual Assault Incident Database."

2. Responsible official: Ms. Darlene Sullivan, Defense Sexual Assault Incident Database Program Manager, 4800 Mark Center Drive, Alexandria, VA 22350-8000, telephone (571) 372-7867.

3. Nature of proposed changes for the Office of the Secretary of Defense to the system: The Office of the Secretary of Defense proposes to alter this system of records by changing the following sections: system location, categories of individuals, categories of records, authority for maintenance of the system, purpose(s), routine uses, safeguards, and record source categories.

4. Authority for the maintenance (maintained, collected, used, or disseminated) of the system: 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.

5. Provide the agency's evaluation on the probable or potential effects on the privacy of individuals: In updating this SORN, the Sexual Assault Prevention and Response Office reviewed the safeguards established for the system of records to ensure they are compliant with the DoD requirements and are appropriate to the sensitivity of the information stored within the system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information has been established.

6. Is the system, in whole or in part, being maintained,

(maintained, collected, used, or disseminated) by a contractor? Yes.

7. Steps taken to minimize risk of unauthorized access: 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 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. Access is further restricted to authorized users on the Nonsecure Internet Protocol Router Network and with a CAC. In addition, the local drive resides behind a firewall and the direct database cannot be accessed from the outside.

8. Routine use compatibility: 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 be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Disclosure When Requesting Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

Disclosure of Requested Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Office of Personnel Management Routine Use: A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the

purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Disclosure to the Merit Systems Protection Board Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

9. OMB public information collection requirements:
OMB collection required: Yes.
OMB Control Number (if approved): 0704-0483.
Expiration Date (if approved) or Date Submitted to OMB: 09/30/2015.

Provide titles of any information collection requests (e.g., forms and number, surveys, interviews scripts, etc.) contained in the systems of records. DD Form 2910, “Victim Reporting Preference Statement” and DD Form 2965, “Defense Sexual Assault Incident Database (DSAID) Data Form.”

In collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A.

10. Name of IT system (state NONE if paper records only): DITPR # 11499, Defense Sexual Assault Incident Database.

DHRA 06

System name:
Defense Sexual Assault Incident Database (November 21, 2012, 77 FR 69442).

Changes:

* * * * *

System location:
Delete entry and replace with “Washington Headquarters Services (WHS), Enterprise Information Technology Support Directorate, 1155 Defense Pentagon, Washington, DC 20301-1155.”

* * * * *

Categories of individuals covered by the system:
Delete entry and replace with “Individuals who may be victims and/or alleged perpetrators in a sexual assault involving a member of the Armed Forces, including: Active duty Army, Navy, Marine Corps, and Air Force members; active duty Reserve members and National Guard members covered by title 10 or title 32 (hereafter ‘service members’); service members who were victims of a sexual assault prior to enlistment or commissioning; military dependents age 18 and older; DoD civilians; DoD contractors; other Federal government employees; U.S. civilians; and foreign military members who may be lawfully admitted into the U.S. or who are not covered under the Privacy Act.”

Categories of records in the system:
Delete entry and replace with “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 perpetrator 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; and any related data on allegations of retaliation associated with reports of sexual misconduct. 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 management includes: 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."

Authority for maintenance of the system:
Delete entry and replace with "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."

Purpose(s):
Delete entry and replace with "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 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."

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Delete entry and replace with "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 be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Disclosure When Requesting Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

Disclosure of Requested Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed

to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Office of Personnel Management Routine Use: A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Disclosure to the Merit Systems Protection Board Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such

other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx"

* * * * *

Retrievability:
Delete entry and replace with "Victim records are retrieved by first name, last name, identification number and type of identification provided, and/or Defense Sexual Assault Incident Database control number assigned to the incident.

Alleged perpetrator records are retrieved by first name, last name, and/or identification number and type of identification provided."

Safeguards:
Delete entry and replace with "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 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. Access is further restricted to authorized users on the Nonsecure Internet Protocol Router Network and with a CAC. In addition, the local drive resides behind a firewall and the direct database cannot be accessed from the outside."

* * * * *

Record source categories:
Delete entry and replace with "Individuals, SARCs, Military Service Legal Officers (i.e. attorneys provided access to the system), Army Law Enforcement Reporting and Tracking System (Army), Consolidated Law Enforcement Operations Center (Navy), and Investigative Information Management System (Air Force)."

* * * * *

DHRA 06 DoD

System name:
Defense Sexual Assault Incident Database.

System location:
Washington Headquarters Services (WHS), Enterprise Information Technology Support Directorate, 1155 Defense Pentagon, Washington, DC 20301-1155.

Categories of individuals covered by the system:
Individuals who may be victims and/or alleged perpetrators in a sexual assault involving a member of the Armed Forces, including: Active duty Army, Navy, Marine Corps, and Air Force members; active duty Reserve members and National Guard members covered by title 10 or title 32 (hereafter 'service members'); service members who were victims of a sexual assault prior to enlistment or commissioning; military dependents age 18 and older; DoD civilians; DoD contractors; other government civilians; U.S. civilians; and foreign military members who may be lawfully admitted into the U.S. or who are not covered under the Privacy Act.

Categories of records in the system:
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; and any related data on allegations of retaliation associated with reports of sexual misconduct. Additional victim and alleged perpetrator 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 management includes: 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.

Authority for maintenance of the system:
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.

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.

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.

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 be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Disclosure When Requesting Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

Disclosure of Requested Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an

individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Office of Personnel Management Routine Use: A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Disclosure to the Merit Systems Protection Board Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a

risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx"

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Paper file folders and electronic storage media.

Retrievability:
Victim records are retrieved by first name, last name, identification number and type of identification provided, and/or Defense Sexual Assault Incident Database control number assigned to the incident.

Alleged perpetrator records are retrieved by first name, last name, and/or identification number and type of identification provided.

Safeguards:
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 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 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. Access is further

restricted to authorized users on the Nonsecure Internet Protocol Router Network and with a CAC.. In addition, the local drive resides behind a firewall and the direct database cannot be accessed from the outside.

Retention and disposal:
Records are cut off at the end of the fiscal year and destroyed fifty years after cut off.

System manager(s) and address:
Sexual Assault Prevention and Response Office, ATTN: Defense Sexual Assault Incident Database Program Manager, 4800 Mark Center Drive, Alexandria, VA 22350-8000.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the appropriate Service office listed below:

The Department of the Army, Human Resources Policy Directorate (HRPD), Sexual Harassment/Assault Response and Prevention (SHARP), 2530 Crystal Drive, 6th Floor, Arlington, VA 22202-3938.

The Department of the Navy, ATTN: Sexual Assault Prevention and Response Program Manager, 716 Sicard Street S.E., Suite 1000, Washington Navy Yard, DC 20374-5140.

Headquarters United States Air Force/A1S, ATTN: Sexual Assault Prevention and Response Program Manager, 1040 Air Force Pentagon, Washington, DC 20330-1040.

The National Guard Bureau, Sexual Assault Prevention and Response Office, ATTN: Sexual Assault Prevention and Response Program Manager, 111 South George Mason Drive, AH2, Arlington, VA 22204-1373.

Signed, written requests should contain the name, identification number and type of identification, and indicate whether the individual is a victim or alleged perpetrator.

Record access procedures:
Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the following as appropriate:

The Department of the Army, HRPD, Sexual Harassment/Assault Response and Prevention (SHARP), 2530 Crystal Drive, 6th Floor, Arlington, VA 22202-3938.

The Department of the Navy, ATTN: Sexual Assault Prevention and Response Program Manager, 716 Sicard Street S.E., Suite 1000, Washington Navy Yard, DC 20374-5140.

Headquarters United States Air Force/A1S, ATTN: Sexual Assault Prevention and Response Program Manager, 1040 Air Force Pentagon, Washington, DC 20330-1040.

The National Guard Bureau, Sexual Assault Prevention and Response Office, ATTN: Sexual Assault Prevention and Response Program Manager, 111 South George Mason Drive, AH2, Arlington, VA 22204-1373.

Signed, written requests should contain the name, identification number and type of identification, indicate whether the individual is a victim or alleged perpetrator, and the number of this system of records notice.

Contesting record procedures:
The OSD rules for accessing records for contesting contents and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 Code of Federal Regulations part 311; or may be obtained from the system manager.

Record source categories:
Individual, SARCs, Military Service Legal Officers (i.e. attorneys provided access to the system), Army Law Enforcement Reporting and Tracking System (Army), Consolidated Law Enforcement Operations Center (Navy), and Investigative Information Management System (Air Force).

Exemptions claimed for the system:
None.