BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2019-OS-0114]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice of a modified System of Records.

SUMMARY: The Office of the Secretary of Defense (OSD) is modifying a System of Records titled, "Defense Sexual Assault Incident Database (DSAID)," DHRA 06 DoD. DSAID is a centralized case-level database, which collects and maintains information on sexual assaults involving Armed Forces members. DSAID gives Sexual Assault Response Coordinators (SARCs) the enhanced ability to provide comprehensive and standardized victim case management.

DSAID is funded and operated by the Department of Defense Sexual Assault Prevention and Response Office (DoD SAPRO) and enables service SAPR Programs to meet congressional reporting requirements and ensure transparency of sexual assault-related data.

DATES: These modifications are effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

SUPPLEMENTARY INFORMATION: DoD SAPRO represents the Secretary of Defense as the central authority charged with preventing sexual assault in the military and facilitating recovery for survivors. DoD SAPRO promotes military readiness by reducing sexual assault through advocacy and execution of program policy, planning, and oversight across the DoD community.

To meet the expanded sexual assault and response reporting requirements of Section 543 of the National Defense Authorization Act for Fiscal Year 2017 (10 U.S.C. 1561) as well as establish the DSAID File Locker, the OSD is modifying this System of Records by changing the following sections: system location, purpose(s) of the system, categories of individuals covered by the system, categories of records in the system, routine use of records maintained in the system, records access procedures, and notification procedures. The DoD notices for Systems of

Records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at http://dpcld.defense.gov/. The proposed systems reports, as required by the Privacy Act, as amended, were submitted on August 7, 2019, to the House Committee on Oversight and Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 of OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated: October 4, 2019.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Defense Sexual Assault Incident Database (DSAID), DHRA 06 DoD.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Washington Headquarters Services (WHS), 1155 Defense Pentagon, Washington, DC 20301-1155.

SYSTEM MANAGER(S): Defense Sexual Assault Incident Database Program Manager, 4800 Mark Center Drive, Alexandria, VA 22350-8000, email: whs.mc-alex.wso.mbx.SAPRO@mail.mil; telephone: (571) 372-2657.

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, 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 1752.5B, SAPR Program; Air Force Instruction 90-6001, SAPR Program; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF 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. 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 to these forms for potential use in Department of Veterans Affairs (DVA) benefits applications.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: 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; 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. Sexual assault victims, family members, bystanders, witnesses, first responders, or other parties (e.g., co-workers and friends) who report (hereafter "retaliation reporters"), and/or are the alleged perpetrators of (hereafter "alleged retaliators") retaliation related to reports of 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"); DoD civilians; and other Federal government employees.

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); 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 identifible 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; gender, 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.

RECORD SOURCE CATEGORIES: 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).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

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:

a. To permit the disclosure of records of closed cases of Unrestricted Reports to the DVA for purpose of providing mental health and 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.

b. To contractors responsible for performing or working on contracts for the DoD when necessary to accomplish an agency function related to this System of Records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure that apply to DoD officers and employees.

c. 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.

d. 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.

e. 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.

f. 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.

g. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the System of Records; (2) the DoD has determined that 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.

h. 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: Paper file folders and electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: For Unrestricted Reports: Victim and retaliation reporter records are retrieved by first name, last name, identification number and type of identification provided, DSAID control number, and/or retaliation control number assigned to the incident. Alleged perpetrator or retaliator

records are retrieved by first name, last name, and/or identification number and type of identification provided. For Restricted Reports: Victim Preference Reporting Statements and SAFE Reports are retrieved by year of report, SARC's assigned location, DSAID Control Number, and/or SARC affiliation, as well as victim answers to the encryption key questions (last four of the SSN, date of birth, and mother's maiden name or state/country of birth) for Restricted Reports.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Temporary. Cutoff cases at the end of the fiscal year and destroy 50 years thereafter.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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 (CAC) and password. Access rights and permission lists for SARCs are granted by Military Service Sexual Assault Prevention and Response program managers through the assignment of appropriate user roles. Access rights and permission lists for authorized military Service Legal Officer and Program Managers are granted by the 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. 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 of it. Victim Preference Statements and SAFE Reports associated with Restricted Reports are also protected by system

administrative roles, and by document level encryption, where victims are able to provide encryption key data.

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, Sexual Harassment/Assault Response and Prevention (SHARP), 2530 Crystal Drive, 6th Floor, Arlington, VA 22202-3938. Headquarters Marine Corps Sexual Assault Prevention and Response, ATTN: SAPR Program Manager, 3280 Russell Road Quantico, VA 22134. The Department of the Navy, ATTN: SAPR Program Manager, RM 4R140-006, 701 S. Courthouse Road, Arlington, VA 22204. Headquarters United States Air Force/A1Z/R, ATTN: SAPR Program Manager 3NW410A, 7700 Arlington Blvd. Falls Church, VA 22042. The National Guard Bureau, SAPR Office, ATTN: SAPR 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, retaliation reporter, alleged perpetrator, or alleged retaliator, and the name and number of this System of Records notice. 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 DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310, 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 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. Headquarters Marine Corps Sexual Assault Prevention and Response, ATTN: SAPR Program Manager, 3280 Russell Road Quantico, VA 22134. The Department of the Navy, ATTN: Sexual Assault Prevention and Response Program Manager, RM 4R140-006, 701 S. Courthouse Road, Arlington, VA 22204. Headquarters United States Air Force/A1Z, 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, retaliation reporter, alleged perpetrator, or alleged retaliator, and the name and number of this System of Records Notice. 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: November 04, 2015, 80 FR 68302.

[FR Doc. 2019-22078 Filed: 10/8/2019 8:45 am; Publication Date: 10/9/2019]