Annual Burden Hours: 3,084.

Needs and Uses: Section 22 of the Arms Export Control Act (22 U.S.C. 2762) requires the U.S. Government to use foreign funds, rather than U.S. appropriated funds, to purchase military equipment for foreign governments. To comply with this requirement, the Government needs to know how much of each progress payment to charge each country. DFARS 232.502–4–70(a) prescribes use of the contract clause at DFARS 252.232–7002, Progress Payments for Foreign Military Sales Acquisitions, in any contract that provides for progress payments and contains FMS requirements. The clause at 252.232–7002 requires each contractor whose contract includes foreign military sales (FMS) requirements to submit a separate progress payment request for each progress payment rate and to submit a supporting schedule that clearly distinguishes the contract's FMS requirements from U.S. requirements. The Government uses this information to determine how much of each country's funds to disburse to the contractor.

Jennifer D. Johnson,

Editor/Publisher, Defense Acquisition Regulations System.

[FR Doc. 2024–30329 Filed 12–19–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2024–OS–0138]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, Department of Defense (DoD).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of the Secretary of Defense is modifying and reissuing a current system of records titled, ''Defense Sexual Assault Incident Database,'' DHRA 06. This system of records was originally established 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; and 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. Additional laws and policy changes require DSAID to include information on the claims of retaliation connected with Unrestricted Reports of sexual assault made by or against a member of the Armed Forces and Unrestricted Reports of adult sexual assault cases under the Family Advocacy Program (FAP). This system of records notice (SORN) is being updated to comply with the National Defense Authorization Act (NDAA), provide the ability to collect sexual assault cases for the U.S. Space Force (USSF), and improve prevention. This SORN is also being updated to add three standard DoD routine uses (routine uses B, I, and J), and various other sections within the SORN to improve clarity or update information that has changed. Additionally, the DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the **Federal Register**.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before January 21, 2025. The Routine Uses are effective at the close of the comment period.

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

* *Federal Rulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox #24, Suite 05F16, 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 *https://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Samuel M. Peterson, DHRA Component Privacy Officer, 400 Gigling Rd., Rm. DODC–MB 7028, Seaside, CA 93955, *dodhra.mc-alex.dhra-hq.mbx.privacy@mail.mil* or 831–220–7330.

SUPPLEMENTARY INFORMATION:

I. Background

The Defense Sexual Assault Incident Database (DSAID) system of records is used to collect and maintain information regarding sexual assaults, and any associated retaliation allegations, involving a member of the Armed Forces. Section 563 of the Duncan Hunter NDAA for Fiscal Year (FY) 2009 (Pub. L. 110–417) requires the DSAID for the purpose of collecting and maintaining information regarding sexual assaults involving a member of the Armed Forces. Additional laws and policy changes require DSAID to include information on the claims of retaliation connected with Unrestricted Reports of sexual assault made by or against a member of the Armed Forces and Unrestricted Reports of adult sexual assault cases under the FAP. As mandated, this Department-wide database includes sexual assault-related data about the victim, the (alleged) offender, and the outcome of any investigation and legal proceedings connected with the assault, or associated retaliation allegation. This SORN is being updated to comply with section 538 of the FY18 NDAA (Pub. L. 115–191) and provide the ability to collect sexual assault cases for the USSF. This SORN is also being updated to add three additional standard DoD routine uses, and various other sections of the SORN.

Subject to public comment, the Office of the Secretary of Defense proposes to update this system of records to add DoD standard routine uses B, I, and J. Modifications are also being made to the following sections of the SORN: (1) to the System Location to add information about cloud storage; (2) to the Authority for Maintenance of the System section to add additional authorities; (3) to the Purpose of the System section to expand on the uses of the information; (4) to the Categories of Records in the System section to clarify the different record types; (5) to the Record Source Categories to add additional source information; (6) to the Policies and Practices for Storage of Records to update the records storage medium in which the records are maintained; (7) to the Policies and Practices for Retrieval of Records to expand on how records are retrieved; (8) to the Administrative, Technical, and Physical Safeguards to update the individual safeguards protecting the personal information; and (9) to the Record Access and Notification Procedures sections to reflect the need for individuals to identify the appropriate DoD office or component to which their request should be directed.

DoD SORNs have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Privacy and Civil Liberties Directorate website at *https://dpcld.defense.gov.*

II. Privacy Act

Under the Privacy Act, a ''system of records'' is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or another identifier assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A–108, the Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency has provided a report of this system of records to the OMB and to Congress.

Dated: December 12, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

Defense Sexual Assault Incident Database (DSAID), DHRA 06.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Washington Headquarters Services (WHS), 1155 Defense Pentagon, Washington, DC 20301–1155. Information may also be stored within a government-certified cloud, implemented, and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301–6000.

SYSTEM MANAGER(S):

Defense Sexual Assault Incident Database Program Manager, 4800 Mark Center Drive, Alexandria, VA 22350–8000, 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; 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; section 543 of Public Law 113–291; DoD Instruction (DoDI) 5505.18, ''Investigation of Adult Sexual Assault in the Department of Defense''; DoDI 6495.02 volume 1 ''Sexual Assault Prevention and Response: Program Procedures; DoD Directive 6495.01, SAPR Program; DoDI 6495.02, SAPR Program Procedures; 32 CFR part 103, SAPR Program, Army Regulation 600–20, chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); OPNAV Instruction 1752.1C, SAPR Program; Marine Corps Order 1752.5BC, SAPR Program; Air Force Instruction 90–6001, SAPR Program; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

A. 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.

B. 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.

C. To facilitate Unrestricted Reports to Congress on the adult sexual assault cases reported by the Family Advocacy Program (FAP).

D. To facilitate use of the ''Catch a Serial Offender'' (CATCH) program in accordance with section 543 of Public Law 113–291, DoDI 5505.18, ''Investigation of Adult Sexual Assault in the Department of Defense'', and DoDI 6495.02 volume 1 ''Sexual Assault Prevention and Response: Program Procedures.''

E. To facilitate the documentation of disclosures of sexual assault and retaliation by covered individuals and questions by interested parties.

F. To facilitate capturing disclosures of and questions regarding sexual assault and retaliation resulting in SAPR-Related Inquiries.

G. To ensure appropriate monthly and quarterly case management and high-risk response team coordination and collaboration to support victim care and case management to include the disclosure of information for the purpose of improving the systemic processes and procedures provided to Service members, and the disclosure of sensitive information for the purpose of providing mental and medical care to Service members during a period of crisis, and/or addressing a high-risk situation, related to an unrestricted report of sexual assault and any associated retaliation reporting.

H. To maintain Victim Reporting Preference Statements, DoD Sexual Assault Forensic Examinations (SAFEs), Retaliation Reporting Statements, requests for the return of a victim's personal property in restricted reports collected during a SAFE, and CATCH Program Explanation and Notification Information for Sexual Assault Victims to ensure compliance with federal records retention requirements, and allow victims and reporters access to these forms for potential use in Department of Veterans Affairs (DVA) benefits applications.

I. 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.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Victims and/or alleged perpetrators in a sexual assault involving a member of the Armed Forces, including: Active duty Army, Navy, Marine Corps, Air Force, and Space 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 civilian employees; 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.

B. 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, Air Force and Space Force members; active duty Reserve members and National Guard members covered by title 10 or title 32 (hereafter ''service members''); DoD civilian employees; and other Federal Government employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal Information such as: Name, DoD ID number, Social Security Number (SSN), and other identification type and number (*e.g.,* passport; U.S. Permanent Residence Card, foreign identification, DSAID control number (*i.e.,* system generated unique control number); date of birth, place of birth, citizenship/immigration status, race/ethnicity, duty status, service, grade/rank, status, occupation, and affiliation (*e.g.,* military, DoD civilian/contractor, other government employee, and military dependent).

B. Victim and alleged perpetrator information may also include: Age at the time of incident, location of incident, and relationship to alleged perpetrator, as applicable. 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.

C. 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.

D. 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 forensic examination performed, and referrals to appropriate resources, information online of duty determinations, victim safety assessment information, case management meeting information (Monthly and Quarterly meetings), High-Risk Response Team Meetings, and information on memoranda of understanding. For Unrestricted Reports, information on expedited transfers and civilian/military protective orders may also be collected.

E. Retaliation reporter and alleged retaliator information may also include: retaliation control number (*i.e.,* system generated unique control number). Other retaliation data collected to support case and business management include: 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.

F. Records maintained for the DSAID File Locker include: Victim Reporting Preference Statement, SAFE reports, year and month of report, Sexual Assault Response Coordinator's (SARC's) assigned location, installation name, DSAID control number, and/or SARC affiliation may be maintained as metadata.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: 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), Investigative Information Management System (Air Force), and Office of Special Investigations (OSI) Records, Investigations & Operations Network (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 under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD pursuant to 5 U.S.C. 552a(b)(3) and the routine uses listed below. (Due to the legal and policy limitations on dissemination of information in restricted reports, not all of the below routine uses may be available for each record or item of information maintained in this system.)

A. 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. 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.

B. 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.

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 confirms a breach of the system of records; (2) the DoD determines 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.

I. To another Federal, State, or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. To permit the disclosure of records of closed cases of Unrestricted Reports to the Department of Veterans Affairs (DVA) for the 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by:

A. 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.

B. 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.

C. For individuals inquiring into the availability of information on sexual assault and retaliation reporting processes and resources under the SAPR program: CATCH Program Explanation and Notification Information for Sexual Assault Victims are retrieved by DSAID Control Number as well as victim answers to the encryption key.

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:

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 SAPR Program Managers are granted by the DSAID Program Manager through the assignment of appropriate user roles. The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures that support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES:

Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the following, as appropriate:

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

B. Headquarters Marine Corps Sexual Assault Prevention and Response, ATTN: SAPR Program Manager, 3280 Russell Road, Quantico, VA 22134.

C. The Department of the Navy, ATTN: SAPR Program Manager, RM 4R140–006, 701 S Courthouse Road, Arlington, VA 22204.

D. Headquarters United States Air Force/A1Z, Integrated Resilience. ATTN: Sexual Assault Prevention and Response Program Manager, 1040 Air Force Pentagon, 5E960, Washington, DC 20330–1040.

E. The National Guard Bureau, SAPR Office, ATTN: SAPR Program Manager, 111 South George Mason Drive, AH2, Arlington, VA 22204–1373.

F. The United States Space Force, ATTN: SAPR Program Manager, 150 Vandenberg St., Suite 3324, Peterson AFB, CO 80914.

Signed, written requests should contain the name and number of this system of records notice along with name, current address, email address of the individual, identification number and type of identification, and indicate whether the individual is a victim, retaliation reporter, alleged perpetrator or alleged retaliator. 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 appropriate 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 follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4); (e)(1), (4)(G), (H), and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(2), as applicable. In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records from which they were a part and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310.

HISTORY:

October 9, 2019, 84 FR 54127; November 04, 2015, 80 FR 68302.

[FR Doc. 2024–29917 Filed 12–19–24; 8:45 a.m.]

BILLING CODE 6001–FR–P

DEPARTMENT OF EDUCATION

[Docket No.: ED–2024–SCC–0125]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Income Based Repayment—Notifications

AGENCY: Federal Student Aid (FSA), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing an extension without change of a currently approved information collection request (ICR).