

records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, email address of the individual, SSN and/or DoDI-ID number, dates of confinement, date of birth, and any details which may assist in locating the records. 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:

Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

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) and (4), (d)(1), (2), (3), and (4); (e)(1), (2) (3), (4)(G)–(I), (5), and (8); (f) and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (j)(2), as applicable. 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. 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 systems of records from which they were a part and claims any additional exemptions set forth here.

HISTORY:

None.

[FR Doc. 2024–29640 Filed 12–20–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2024–OS–0143]

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 DoD is modifying a system of records titled, "Joint Advertising, Market Research & Studies Recruiting Database (JAMRS)," DHRA 04. The JAMRS Recruiting Database compiles, processes, and distributes files of individuals, ages 16 to 18 years, to the Services to assist them in their direct marketing recruiting efforts. This system of records notice (SORN) is being updated to add two new DoD Standard routine uses (Routine Uses I and J) which authorize disclosures to allow for coordination with the Office of Inspector General and other disclosures mandated by Federal statute or treaty. The DoD is also modifying various other sections within the SORN to improve clarity or update information that has changed.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before January 22, 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 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 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 <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT:

Samuel 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 JAMRS Recruiting Database serves as a centralized database used to compile, process, and distribute files of individuals, ages 16 to 18 years, to the Services to assist them in their direct marketing recruiting efforts. Subject to public comment the OSD is updating this SORN to add two new DoD Standard routine uses (Routine Uses I and J) which authorize disclosures to allow for coordination with the Office of Inspector General and other disclosures mandated by Federal statute or treaty. In addition to updating the routine use section, the other modifications are to the following sections: (1) System Location to update the address, (2) Authority for Maintenance of the System to update citation(s); (3) Purpose of the System to improve clarity; (4) Categories of Records to provide clarity; (5) Records Source Categories to add additional sources; (6) Policies and Practices for Storage of Records to account for the use of Government-validated Cloud Computing environments; (7) Policies and Practices For Retrieval of Records for clarity; (8) Administrative, Technical, and Physical Safeguards to update the description of safeguards protecting these records; (9) to the Record Access, Notification, and Contesting Record Procedures, to reflect the updated guidance for accessing records and to update the appropriate citation for contesting records. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

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://dpcl.d.defense.gov/privacy>.

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 other identifying particular 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, OATSD(PCLT) has provided a report of

this system of records to the OMB and to Congress.

Dated: December 18, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

Joint Advertising, Market Research & Studies Recruiting Database (JAMRS), DHRA 04.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. 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):

Program Manager, Defense Personnel Analytics Center, Office of People Analytics, Joint Advertising, Market Research & Studies (JAMRS), Suite 06J25, 4800 Mark Center Drive, Alexandria, VA 22350-4000; email: info@jamrs.org.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 503(a), Enlistments: recruiting campaigns; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 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; and 14 U.S.C. 350 Coast Guard, and E.O. 9397 as amended.

PURPOSE(S) OF THE SYSTEM:

The Joint Advertising, Market Research & Studies (JAMRS) Recruiting Database is to compile, process and distribute files of individuals, ages 16 to 18 years, and to the Services to assist them in their direct marketing recruiting efforts. The system also provides JAMRS with the ability to measure effectiveness of list purchases through ongoing analysis and to remove the names of individuals who are current/former members of, or are enlisting in, the Armed Forces, and individuals who have asked to be removed from consideration as a participant in any future recruitment lists.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Individuals aged 16 to 18; college students; Selective Service System registrants; individuals who have taken

the Armed Services Vocational Aptitude Battery (ASVAB) test; individuals who have responded to various paid/non-paid advertising campaigns seeking enlistment information; current military personnel who are on Active Duty or in the Reserves and prior service individuals who still have remaining Military Service Obligation; individuals who are in the process of enlisting.

B. Individuals who have asked to be removed from any future recruitment or marketing lists via direct request, enrollment in do not mail registries, or death. Opt-Out information:

Individuals, who are 15½ years old or older, or parents or legal guardians acting on behalf of individuals who are between the ages of 15½ and 18 years old, seeking to have their name or the name of their child or ward, as well as other identifying data, removed from this system of records (or removed in the future when such information is obtained) should address written Opt-Out requests to the Joint Advertising, Marketing Research & Studies (JAMRS), ATTN: Opt-Out, Suite 06J25, 4800 Mark Center Drive, Alexandria, VA 22350-4000. Such requests must contain the full name, date of birth, and current address of the individual. Opt-Out requests will be honored for ten years. However, because Opt-Out screening is based, in part, on the current address of the individual, any change in address will require the submission of a new Opt-Out request with the new address.

CATEGORIES OF RECORDS IN THE SYSTEM:

Personal information may include, name, DoD ID number, date of birth, ethnicity, gender, email and mailing address, city, state, zip code, source code, telephone number, education level, military status, selective service registration method.

A. For individuals aged 16 to 18 years: high school name, graduation date, grade point average, education level, military interest, college intent, ethnicity, ASVAB test date, and ASVAB Armed Forces Qualifying Test Category Score.

B. For college students: college name, college location, college type, college competitive ranking, class year, and field of study.

C. Individuals who have responded to various paid/non-paid advertising campaigns seeking enlistment information: Service Code, and contact immediately flag.

D. For military personnel: application date, military service, and occupation information.

E. Opt-Out: For individuals who have asked to be removed from future

recruitment or marketing lists: reason code.

Note: Individuals who have submitted an opt-out request to JAMRS, the system maintains the individuals' information in suppression files. The suppression files ensure those individuals are not contacted.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: The Individual; State Department of Motor Vehicle offices; commercial information brokers/vendors; Selective Service System; Defense Manpower Data Center; United States Military Entrance Processing Command for individuals who have taken the ASVAB test; and the Military services, Congressional offices, and the Direct Marketing Association for individuals who have asked to be removed from any future recruitment lists.

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 as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

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 the Department of Homeland Security to support outreach efforts targeted at prospective United States Coast Guard recruits.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically in secure facilities behind a locked door. Electronic records may be stored locally on 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 name, address, and date of birth.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Destroy three years from the date the information pertaining to the individual is first distributed to the Services or, or from the date on which the file has been inactive for one year, according to the mail usage dates, as appropriate.

Contact information of individuals who wish to be removed (Opt-Out suppression files) is retained for ten (10) years from the date the information is added.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to information in the database is highly restricted and limited to those that require the records in the performance of their official duties. Personnel with access to the database have completed background security checks and have been provided Command Access Cards. The database complies with DoD cloud computing policy and procedural guidance as published. The database utilizes a layered approach of overlapping controls, monitoring, and authentication to ensure overall security of the data, network, and system resources. The use of information security continuous monitoring supports the maintenance of ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Sophisticated physical security, perimeter security (firewall, intrusion prevention), access control, authentication, encryption, data transfer, and monitoring solutions prevent unauthorized access from internal and external sources. The following administrative controls are also applied to restrict access to those who require the data in the performance of their official duties: periodic security audits; regular monitoring of users' security practices; methods to ensure only authorized personnel have access to personally identifiable information; encryption of backups containing sensitive data; and backups secured offsite.

RECORD ACCESS PROCEDURES:

Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Parents and guardians of minor children must follow the procedures in 32 CFR 310.3(d) to obtain access to records of the child. These

procedures require the parent or legal guardian to establish: (1) The identity of the individual who is the subject of the record; (2) the parent/guardian's own identity; (3) that the requester is the parent or guardian of that individual, which may be proven by providing a copy of the individual's birth certificate showing parentage or a court order establishing the guardianship; and (4) that the parent or guardian is acting on behalf of the individual in making the request. Individuals should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed, written requests should contain the name and number of this system of records notice and the name, date of birth, and current address of the individual. 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, for contesting contents, and for 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:

None.

HISTORY:

October 16, 2019, 84 FR 55292;
December 22, 2011, 76 FR 79663.

[FR Doc. 2024-30611 Filed 12-20-24; 8:45 am]

BILLING CODE 6001-FR-P