PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Advertising, Market Research and Studies Recruitment Database and Survey Database
Defense Human Resources Activity

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	13132
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DHRA 04, DHRA 05

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Authority for maintenance of the system (DHRA 04) :
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. 3013 (Secretary of the Army); 10 U.S.C. 5013 (Secretary of the Navy); 10 U.S.C. 8013 (Secretary of the Air Force); and E.O. 9397 (SSN).
Authority for maintenance of the system (DHRA 05) :
U.S.C. Title 10 Section 503(a): Enlistments: recruiting campaigns; 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); and 10 U.S.C 2358, Research and development projects.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Joint Advertising, Market Research & Studies (JAMRS) Recruiting Database
The purpose of the JAMRS Recruiting Database is to compile, process and distribute files of individuals 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 currently members of, or are enlisting in, the Armed Forces or who have asked that their names be removed from future recruitment lists.
The types of personal information collected in the system include: All Records: Full name, gender, address, city, state, zip code and list source code. JAMRS based on list sources also collect on a limited basis: For young Adults aged 16 to 18; Date of birth, telephone number, high school name, graduation date, grade point average, education level, military interest, college intent, ethnicity, ASVAB test date, ASVAB Armed Forces Qualifying Test Qualifying Score. For College Students: telephone number, college name, college location, college type, college competitive ranking, class year, ethnicity, field of study. For Selective Service System: Date of birth, scrambled Social Security Number, Selective Service registration method. Individuals who have responded to various paid/non-paid advertising campaigns seeking enlistment information: Date of birth, telephone number, Service Code, last grade completed, email address, contact immediately flag. For Military Personnel: Date of birth, Scrambled Social Security Number, ethnicity, education level, application date, military service and occupation information. For individuals who have asked to be removed from future recruitment list: Date of birth, reason code.

Joint Advertising, Market Research & Studies (JAMRS) Survey Database
The purpose of the JAMRS Survey Database is to compile names of young adults aged 16 through maximum recruiting age to create a mailing frame from which to conduct surveys. These surveys will be conducted multiple times a year and each survey will be designed so that appropriate levels of precision can be achieved for inferences to be made at various geographic levels. The system also provides JAMRS with the ability 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 JAMRS survey.

Identifiable information across all sources will include name, gender, ethnicity (when available) address, city, state and zip. A scrambled social security number will be utilized in a very limited way for current military personnel who are on Active Duty or in the Reserve components; prior service individuals who still have remaining Military Service Obligation; and records obtained from Selective Service System.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risk to an individual would be having an unauthorized person gaining access to their contact information.

Due to the sensitive information collected on individuals, the contractor has established a highly secure and restrictive environment by putting in place appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the system. Vulnerability and risk assessment reviews are conducted on a regular basis to ensure maximum safeguarding of information. In addition, JAMRS maintains accreditation under Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) with initial authority to operate (ATO) granted on 1 October 2010 with annual reviews.

Access to the database(s) is highly restricted and limited to those that require the records in the performance of their official duties. The Database(s) utilizes a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the data, network and system resources.

Sophisticated physical security, perimeter security (firewall, intrusion protection), access control, authentication, encryption, data transfer, and monitoring solutions prevent unauthorized access from internal and external resources.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. JAMRS Program Manager, JAMRS Chief Joint Advertising, and the JAMRS Direct Marketing Project Officer.

☒ **Other DoD Components.**

Specify. Air Force, Air Force Reserve, Army, Army National Guard, Army Academy/ ROTC, Army Reserve, Coast Guard, Coast Guard Academy, Marines, Navy, and Navy Reserves.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. The contract includes the Privacy Act clause of the Federal Acquisition Regulation (FAR), specifically FAR 52.224-2, under which the contractor/subcontractor agrees to comply with the requirements of the Privacy Act and DoD rules and regulations issued under the Act. This contract provision also treats the contractor/subcontractor as an employee of DoD for purposes of the Privacy Act, and is thus subject to possible criminal penalties if the Act is violated. The contract also incorporates FAR 52.239-1, Privacy and Security safeguards, which includes a notification requirement if new or unanticipated threats or hazards are discovered, or if existing safeguards cease to function.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Because JAMRS collects information through a variety of sources for both Databases, individuals do not have an opportunity to object to the collection of their PII.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

When responding to paid or non-paid advertising, it is understood the individual gives consent to forward their contact information to the Services to receive additional information. JAMRS provides individuals with the opportunity to opt-out of the JAMRS databases. Individuals should address written inquiries to the Joint Advertising, Market Research and Studies (JAMRS), Direct Marketing Program Officer, Suite 06J25, 4800 Mark Center Drive, Alexandria, VA 22350-4000. Opt-out requests should contain the full name, date of birth, and current address of the individual."

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

JAMRS receives data directly from individuals through the following formats for DHRA -04:
Business Reply Cards (BRC's): Information provided on the BRC's to address PII data are as followed:
"Authority: 10 U.S.C. 503 (a), Enlistments: Recruiting Campaigns. Purpose(s): To compile, process and distribute contact information of individuals to the Services to assist them in their direct marketing recruitment efforts. Routine Uses(s): None. Disclosure: Voluntary. However, failure to disclose pertinent information may result in our inability to contact you with further information."

Web Site: Today's Military: Information provided on the Today's Military website to address PII data

are as followed:
"Authority: 10 U.S.C. 503 (a), Enlistments: Recruiting Campaigns. Purpose(s): To compile, process and distribute contact information of individuals to the Services to assist them in their direct marketing recruitment efforts. Routine Uses(s): None. Disclosure: Voluntary. However, failure to disclose pertinent information may result in our inability to contact you with further information."

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.