PRIVACY IMPACT ASSESSMENT (PIA)

For the

GOARMY.COM - GOARMY.COM
US Army Deputy Chief of Staff for Personnel / Human Resources Command (HRC)

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 16519 DA303120

☐ **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 A0601-210 AHRC

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. (1 of 20 systems covered by the above SORN)

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.

10 United States Code (USC) 503, Enlistments: Recruiting Campaigns, Compilation of Directory Information; and 10 USC 3013, Secretary of the Army.

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.

GOARMY.COM is a website that handles electronic recruiting efforts for the United States Army. This website receives over 100 million page views annually and has over 15 million visitors. It handles all accessioning and recruiting missions including the larger active duty, Army Reserve, and Reserve Officer Training Corps missions. GOARMY.COM is the hub of the Army's digital-centric marketing efforts. All marketing material for Army recruiting drives to GOARMY.COM, where prospects are provided a vast range of information about the depth and breadth of serving in the US Army, including up-to-date information on over 150 careers. The ultimate goal of this electronic recruiting tool is to provide prospective recruits the critical information needed for them to make an educated decision about joining the military. These decisions in turn become qualified leads through various activations on the site, including electronic business reply cards, emailing to the US Army Recruiting Command (USAREC) Virtual Recruiting Center, local recruiter contact information, and online applications for both USAREC and the US Army Cadet Command.

Types of PII collected include personal, contact, and education information.

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

The system and its components are maintained in a controlled, secure facility. Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Employees and appropriate contractor personnel are required to obtain security/information assurance training and certification based on system access levels and level of assigned responsibility. Data are passed via secure wide area networks or via use of virtual private networks. Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal.

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. Army Audit Agency, Army Marketing and Research Group, Department of the Army Inspector General, Provost Marshal General, US Army Cadet Command, US Army Criminal Investigation Command, US Army Intelligence and Security Command, and US Army Recruiting Command.

☒ **Other DoD Components.**

Specify. Defense Criminal Investigative Service and Department of Defense Inspector General.

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. McCann Worldwide (MRM) contractual language states: "Updates and/or upgrades the leads database based on emerging security requirements. These updated and/or upgrades shall be implemented immediately as they become identified by the Army or higher authority. The contractor shall also maintain and protect personally identifiable information (PII) maintained in the database, based on current DoD and Army rules and regulations." (C.5.1.6.6.9.) "The contractor shall include security requirements for the operation of fulfillment processes in the current Fulfillment SOP. The contractor shall implement all necessary upgrades and updates to the fulfillment process in accordance with emerging security requirements." (C.5.1.6.7.11.) The system shall include data for lead generation activities and provide lead generation analysis and tracking data consistent with current, evolving advertising industry practices in compliance with DoD and Army security and IT system regulations and guidelines.

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

Specify. N/A

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.

Data are collected directly from individuals, who can object to its collection by refusing to provide it.

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

N/A

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.

Data are collected directly from individuals who consent to its use by providing the data.

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

N/A

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.

The GOARMY.COM website displays the following:

PRIVACY & SECURITY NOTICE
GoArmy.com is committed to protecting your privacy. Therefore, your use and implementation of the information and information request forms included in this Web site are covered under the following guidelines.
1. The United States Army Recruiting Web site (GoArmy.com) is provided as a public service by the Army Marketing and Research Group (AMRG) and the Department of the Army.
2. Information presented on the Army Recruiting Web site is considered public information and may be distributed or copied. Photographs, videos and music require permission for use and remain the property of the United States Army or copyright owner and may not be reproduced except by permission.
3. Privacy Act Notice: Disclosure of any information by you is strictly voluntary. However, delays in providing you requested materials may result by not providing complete information. All information collected will be used strictly for recruiting purposes. The authority for the collection of this information is Title 10, United States Code, Section 503.
4. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
5. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
6. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20.
7. For site navigation purposes only, cookies are used in a limited manner. Cookies are pieces of information that a Web site transfers to your computer's hard disk for record-keeping purposes. Cookies can make the Web more useful by storing information about your preferences on a particular site. The use of cookies is an industry standard, and many major Web sites use them to provide useful features for their customers. Cookies in and of themselves do not personally identify users, although they do identify a user's computer. Most browsers are initially set up to accept cookies. If you'd prefer, you can set yours to refuse cookies. However, you may not be able to take full advantage of a Web site if you do so.

8. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.
9. Penalty for False Statements. The US Criminal Code (Title 18 US Code Section 1001) provides that whoever, in any matter within the jurisdiction of the Government of the United States, knowingly and willfully - (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined or imprisoned not more than 5 years, or both.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☒ Citizenship	☐ Legal Status	☒ Gender
☒ Race/Ethnicity	☒ Birth Date	☐ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal Email Address
☒ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☒ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☒ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.

Additional PII collected includes height, weight, number of dependents, and whether the individual previously served in the military.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Individual.

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☒	**Web Site**
☐	**Information Sharing - System to System**		
☐	**Other**		

N/A

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Identification. Candidates are pre-qualified with the collected information, with the desired end result of a signed enlistment contract.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Administrative use. The information is used by Army recruiters to enlist candidates into the US Army.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

N/A

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other**

N/A

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒ **Security Guards**	☒ **Cipher Locks**
☒ **Identification Badges**	☐ **Combination Locks**
☐ **Key Cards**	☒ **Closed Circuit TV (CCTV)**
☐ **Safes**	☐ **Other**

N/A

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**	☐ **Biometrics**
☒ **Password**	☒ **Firewall**
☐ **Intrusion Detection System (IDS)**	☒ **Virtual Private Network (VPN)**
☒ **Encryption**	☐ **DoD Public Key Infrastructure Certificates**
☐ **External Certificate Authority (CA) Certificate**	☐ **Common Access Card (CAC)**
☐ **Other**	

N/A

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☒ **Other**

Users are required to successfully undergo and complete a National Agency Check with Inquiries along with a credit check. Access to the system is managed by the HRC access control procedures and policies. All aspects of privacy, security, configuration, operations, data retention, and disposal are documented to ensure privacy and security are consistently enforced and maintained.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	Registered Parent Dependencies: DIACAP
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: PII is collected directly from individuals.
Use: PII is used to identify enlistment candidates and to provide leads to recruiters.
Retention: PII is securely maintained by GOARMY.COM and has up to a 20-year retention period.
Processing: GOARMY.COM processes PII in order to provide current information on Army careers to potential enlistees so they can make informed decisions, and to provide information on enlistment candidates to recruiters and to USACC and USAREC.
Disclosure: PII is disclosed only to authorized individuals who have a need to know.
Destruction: PII is purged by overwriting when the information is no longer required.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Due to the level of safeguarding identified in Section 3, we believe the risk to individuals' privacy to be minimal.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	DENHUP.PAUL.FRANK.1014582394 Digitally signed by DENHUP.PAUL.FRANK.1014582394 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=DENHUP.PAUL.FRANK.1014582394 Date: 2016.10.24 12:45:29 -04'00'
Name:	Paul F. Denhup
Title:	Program Manager, GOARMY.COM
Organization:	Army Marketing and Research Group
Work Telephone Number:	(703) 545-6186
DSN:	
Email Address:	paul.f.denhup.civ@mail.mil
Date of Review:	2016/10/24
Other Official Signature (to be used at Component discretion)	JOURNEY.ALLAN.DALE.1209947508 Digitally signed by JOURNEY.ALLAN.DALE.1209947508 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=JOURNEY.ALLAN.DALE.1209947508 Date: 2016.10.25 06:49:38 -04'00'
Name:	Allan D. Journey
Title:	Information Systems Security Manager
Organization:	Army Human Resources Command, KNOX-HRC-PSA-AC
Work Telephone Number:	(502) 613-7567
DSN:	983-7567
Email Address:	allan.d.journey.civ@mail.mil
Date of Review:	25 Oct 2016

Other Official Signature (to be used at Component discretion)

WEY.MONIQUE.A.1152083013

Digitally signed by WEY.MONIQUE.A.1152083013
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=WEY.MONIQUE.A.1152083013
Date: 2016.10.31 11:06:23 -04'00'

Name:	Monique A. Wey
Title:	Chief, Freedom Of Information Act Office
Organization:	Army Human Resources Command, KNOX-HRC-FOIA
Work Telephone Number:	(502) 613-4057
DSN:	983-4057
Email Address:	monique.a.wey.civ@mail.mil
Date of Review:	

Component Senior Information Assurance Officer Signature or Designee

ASSI.CAROL.M.1232251189

Digitally signed by ASSI.CAROL.M.1232251189
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=ASSI.CAROL.M.1232251189
Date: 2017.01.27 11:56:56 -05'00'

Name:	Carol M. Assi
Title:	Chief, Cybersecurity Programs Division
Organization:	HQDA CIO/G-6, Cybersecurity Directorate
Work Telephone Number:	703-545-1692
DSN:	865-1692
Email Address:	Carol.m.assi.civ@mail.mil
Date of Review:	27 January 2017

Component Privacy Officer Signature

MORTON.KIMBERLY.P.1229635448

Digitally signed by MORTON.KIMBERLY.P.1229635448
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=MORTON.KIMBERLY.P.1229635448
Date: 2016.12.22 09:30:58 -05'00'

Name:	Kimberly P. Morton
Title:	Army Privacy Officer
Organization:	HQDA/OAA/RMDA/PA
Work Telephone Number:	(703) 428-6211
DSN:	
Email Address:	kimberly.p.morton.civ@mail.mil
Date of Review:	12/22/2016

Component CIO Signature (Reviewing Official)	LUNDGREN.LEROY.1172851556 Digitally signed by LUNDGREN.LEROY.1172851556 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=LUNDGREN.LEROY.1172851556 Date: 2017.01.31 16:23:31 -05'00'
Name:	LeRoy (Roy) Lundgren CISSP
Title:	Deputy Director
Organization:	Army CIO/G6 Cybersecurity Directorate
Work Telephone Number:	703-545-1679
DSN:	865-1679
Email Address:	leroy.lundgren.civ@mail.mil
Date of Review:	31 Jan 17

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.