PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

GOARMY.COM - GOARMY.COM

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

02/01/24

Headquarter Department of Army, Deputy Chief of Staff G-1, Army Enterprise Marketing Office (AEMO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

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

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

GoArmy.com is a website that supports marketing and recruiting efforts for the U.S. Army Active Duty, Army Reserve, Army National Guard, and Reserve Officer Training Corps. The purpose is to provide prospective military recruits the critical information needed to make an educated decision about joining the Army by submitting contact information via email, an electronic Business Reply Cards (eBRC), and the GoArmy.com Contact Center. GoArmy.com generates leads by linking the eBRC with Enterprise Marketing Management System (EMMS) via EMMS Application Programming Interface (API).

GoArmy.com collects Personally Identifiable Information (PII) and transmits to EMMS through encrypted communication. This website does not store PII data.

PII collected includes: citizenship, home and cell phone numbers, mailing home address, place of birth, work email address, date of birth, education information, law enforcement information, marital status, DoD ID, gender/gender identification, legal status, medical information, and names.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is used be for authentication and mission-related use.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Interested military applicants do not have to provide PII online; however, military recruiters may not be able to contact individuals or follow up if the requested information is not provided.

f. 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.

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

Interested military applicants do not have to provide PII online; however, military recruiters may not be able to contact individuals or follow up if the requested information is not provided.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and*

provide the actual wording.)

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

PRIVACY ACT STATEMENT:

AUTHORITY: 10 USC 503: Enlistments: recruiting campaigns; compilation of directory information; 10 USC 504: Persons not qualified; 10 USC 505: Regular components: qualifications, term, grade; 10 USC 508: Reenlistment: qualifications; 10 USC 651: Members: required service; 10 USC 2102: Establishment; 10 USC 7013: Secretary of the Army; and Army Regulation 601-210, Active and Reserve Components Enlistment Program.

PRINCIPLE PURPOSE(s): To respond to inquiries from individuals interested in joining U.S. Army Active Duty, Army Reserve, Army National Guard, and Reserve Officer Training Corps. To determine qualification(s) of prospective recruits. To obtain potential recruits skills, educational, and assignment preferences and objectives. To provided responses to prospective recruit queries. See Army System of Records Notice A0601-210c TRADOC Army Recruiting Prospect System: A0601-210c TRADOC > Privacy, Civil Liberties, and Freedom of Information Directorate > DOD-wide SORN Article View (defense.gov).

ROUTINE USE: None.

DISCLOSURE: Voluntary. However, failure to provide the requested information may hinder the ability to contact individuals and provide additional information about the recruiting process.

Privacy Act Notice: The above disclosure is voluntary. All information will be used strictly for recruiting purposes. The authority for the collection of this information is Title 10, United States Code, Sections 503, 505, 508, and 12102. For more information, please review our Privacy & Security Notice (https://www.goarmy.com/privacy.html).

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	U.S. Army National Guard, U.S. Army Reserve, U.S. Army Recruiting Command, U.S. Army Cadet Command
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	U.S. Air Force Reserve Command, Air Force Recruiting Service, Air National Guard, U.S. Marine Corps, U.S. Navy
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	
☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☒ Website/E-Form

☐ Other *(If Other, enter the information in the box below)*

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier A0601-210c TRADOC

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

SORN listed above is for legacy GoArmy.com and is approved for use. A new DoD-wide SORN is pending publication, DoD-00**, "Accessions."

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 3.1 Item 020, DAA-GRS-2013-0005-0004

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 USC 503: Enlistments: recruiting campaigns; compilation of directory information.
10 USC 505: Regular components: qualifications, term, grade.
10 USC 504: Persons not qualified.
10 USC 508: Reenlistment: qualifications.
10 USC 651: Members: required service.
10 USC 2102: Reserve components: qualifications.
Army Regulation 601-210 Active and Reserve Components Enlistment Program.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

IAW DoDM 8910.01, Vol 2, para 8. b. 13, this type of information collection is not considered public information and therefore does not require processing IAW the Paperwork Reduction Act (PRA). Collection of information is conducted for advertising and market research

targeted at prospective recruits for the Military Services and those who may influence prospective recruits that is intended to enhance the effectiveness of recruiting programs of the DoD in accordance with Section 503(1) of Title 10, United States Code.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☒ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☒ Education Information	☐ Emergency Contact
☐ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☒ Law Enforcement Information	☒ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☒ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☒ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☐ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☐ No

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☐ Cipher Locks
- ☐ Combination Locks
- ☐ Key Cards
- ☐ Security Guards
- ☐ Closed Circuit TV (CCTV)
- ☐ Identification Badges
- ☐ Safes
- ☒ If Other, enter the information in the box below

Hosted in cARMY AWS GovCloud IL4.

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☒ Firewall
- ☒ Role-Based Access Controls
- ☐ Virtual Private Network (VPN)
- ☒ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☐ Used Only for Privileged (Elevated Roles)
- ☐ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☐ External Certificate Authority Certificates
- ☒ Least Privilege Access
- ☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

N/A

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

☒	Yes, DITPR	DITPR System Identification Number	16519/AITR: DA303120
☐	Yes, SIPRNET	SIPRNET Identification Number	
☒	Yes, RMF tool	RMF tool Identification Number	eMASS ID: 4425
☐	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

☒	Authorization to Operate (ATO)	Date Granted:	11/15/2022
☐	ATO with Conditions	Date Granted:	
☐	Denial of Authorization to Operate (DATO)	Date Granted:	
☐	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

Expiration date: 11/14/2025 (Accreditation inherited from RSN - Recruiting Services Network (DA05891)) The system is transitioning and following the Risk Management Framework 2.0 and will obtain an Army ATO by the estimated date, April 2024.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

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

☒ Yes ☐ No

If "Yes," Enter UII 007-000100053 If unsure, consult the component IT Budget Point of Contact to obtain the UII.

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	MAJ David Galbreath	(1) Title	Program Manager
(2) Organization	Army Enterprise Marketing Office (G-1)	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	10/13/23
b. Other Official *(to be used at Component discretion)*	Debra Woods	(1) Title	Program Information Systems Security Manager
(2) Organization	HQDA, G-1, TBAI, GPfM	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	10/22/23
c. Other Official *(to be used at Component discretion)*	Kathleen Vaughn-Burford	(1) Title	Privacy Officer/Records Manager
(2) Organization	HQDA, DCS G-1	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	10/25/23
d. Component Privacy Officer (CPO)	Joyce Luton	(1) Title	Director, Army Records Management Directorate
(2) Organization	CIO/ESA/ARMD	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	01/12/24

e. Component Records Officer	Andrica Dickerson	(1) Title	Army Records Officer, Chief, Records Management Division
(2) Organization	OCIO/ARMD	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	01/05/24
f. Component Senior Information Security Officer or Designee Name	Terry Watson	(1) Title	Authorizing Official
(2) Organization	HQDA, DCS G-1	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	01/03/24
g. Senior Component Official for Privacy (SCOP) or Designee Name	Carrie A McVicker	(1) Title	Executive Director, Enterprise Services Agency (ESA)
(2) Organization	CIO/ESA	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	01/18/24
h. Component CIO Reviewing Official Name	Leonel T. Garciga	(1) Title	Army Chief Information Officer
(2) Organization	HQDA CIO	(3) Work Telephone	[redacted]
(4) DSN	[redacted]	(5) E-mail address	[redacted]
(6) Signature	[redacted]	(7) Date of Review	02/01/24

Publishing: Only Section 1 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: osd.mc-alex.dod-cio.mbx.pia@mail.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 Section 1.