



PRIVACY IMPACT ASSESSMENT (PIA)

For the

GoArmyEd

HQDA G1 - HRC - Human Resource Command

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

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
- 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

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.

Title 10 US Code Sections 3013 (Secretary of the Army) and 4302, Executive Order 9397 as amended (SSN); AR 621-5, Army Continuing Education System; AR 350-1; and AR 690-950.

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.

GoArmyEd is an Army Continuing Education System program that provides the virtual gateway to request Tuition Assistance (TA) online anytime for classroom, distance learning, and online college courses. GoArmyEd is a dynamic online portal that automates many of the paper-based processes historically conducted in-person at Army Education Centers. The system includes automated registration tools that enforce TA policies and procedures. GoArmyEd is used by Soldiers, Department of the Army Civilians, family members, sister services, veterans and authorized users of the education center to pursue their post secondary educational goals and to utilize testing services; Army Education Counselors to provide educational guidance; and colleges to deliver degree and course offerings and to report individual progress. Personal information maintained by the system includes identification data, contact information, military personnel data, and education information.

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

All systems and environments have threats that seek to exploit and cause harm to the information. Some threats are natural, some are inherent in the system design, some can be attributed to unauthorized personnel, and some to authorized personnel who make mistakes. Four general categories of threats exist: human-intentional, human-unintentional, structural, and natural. The system is maintained in a controlled facility that is DIACAP Accredited. The system achieved a DIACAP Accreditation on 2 Jan2011. 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, 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.

Staff principals in the chain of command, the personnel systems supporting Army Human Resources Command, the Army Career Tracker System, the Department of the Army Inspector General, the Army Audit Agency, the US Army Criminal Investigation Command, the US Army Intelligence and Security Command, the Provost Marshall General, and the Assistant Secretary of the Army for Financial Management and Comptroller.

Other DoD Components.

Specify.

The Defense Finance and Accounting Service, the Department of Defense Inspector General, and the Defense Criminal Investigative Service.

Other Federal Agencies.

Specify.

The Department of Veterans Affairs, the Department of Labor, and the Bureau of Apprenticeship and Training.

State and Local Agencies.

Specify.

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

Specify.

Science Applications International Corporation and IBM contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentiality and security of a Soldier's PII. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of a work day. Contractual language directs and requires each SAIC and IBM employee in support of the system to have a valid Secret clearance prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U.S. Code Section 522a, and all applicable agency rules and regulations.

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

Specify.

US Bank and supporting colleges and universities.

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.

Personal data are voluntarily given by the applicant and collected via electronic form on the GoArmyEd web site, and individuals can object to the collection by refusing to complete the forms. The system also extracts information from existing information systems. In those cases, since data are not collected directly from individuals they are not provided either a Privacy Act Statement or a Privacy Advisory for use of that data. However, Soldiers are afforded the opportunity to object to capture and use of that information at the time of employment or enlistment in the Department of the Army.

(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.

Personal data are voluntarily given by the applicant and collected via electronic form on the GoArmyEd web site. A Privacy Act statement describing the agency's practices regarding the specific uses, collection or maintenance of this information is provided to individuals at time of PII collection. The system also extracts information from existing information systems. In those cases, since data are not collected directly from individuals they are not provided either a Privacy Act Statement or a Privacy Advisory for use of that data. However, individuals are afforded the opportunity to consent to the use of that information at the time of

employment or enlistment in the Department of the Army.

(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.

Personal data are voluntarily given by the applicant and collected electronically on the GoArmyEd web site. A Privacy Act statement describing the agency's practices regarding the specific uses, collection or maintenance of this information is provided to individuals at time of PII collection.

"Title 5 USC 301; Title 10 USC 3013 and 4302; Army Regulation 621-5, Army Continuing Education System; and E.O. 9397 authorize the collection of this information. The primary use of this information is to enable the Go Army Education (GoArmyEd) program to provide Army Continuing Education System services. In addition to the general disclosures permitted by the Privacy Act and the Army's systems of records notices, information may be disclosed to the Department of Labor, Bureau of Apprenticeship and Training for individuals enrolled in an Army Apprenticeship Program. Disclosure of the requested information is Voluntary. Failure to provide information may result in the inability to obtain Army Continuing Education System services."

If You Send Us Personal Information: If you choose to provide us with personal information, as in an email to one of our online email boxes, we use that information to respond to your message and to help us get you the information you have requested. We do not collect personal information for any purpose other than to respond to you. We collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you. We only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We do not collect information for commercial marketing.