



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Partnership for Youth Success (PAYS)
--------------------------------------

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
- 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.

10 USC 3013, Secretary of the Army; Army Regulation 601-210, Active and Reserve Components Enlistment Program, and Executive Order 9397 as amended (SSN).

**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.

The Partnership for Youth Success (PAYS) website (www.armypays.com) includes features and functions that support collaboration and information sharing between industry leaders and the Army Recruiting Community. PAYS is sponsored and managed by the Army Marketing and Research Group.

PII collected includes personal and contact data, family data, reference data, travel data, military records, and financial, medical, disability, law enforcement, employment, emergency contact, 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. 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. Department of the Army Inspector General, Army Audit Agency, US Army Criminal Investigation Command, US Army Intelligence and Security Command, Provost Marshal General.

**Other DoD Components.**

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

**Other Federal Agencies.**

Specify. Office of Personnel Management, Selective Service System, Social Security Administration, Department of Justice (FBI).

**State and Local Agencies.**

Specify. N/A

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

Specify. 1. Science Applications International Corporation (SAIC) is the principal contractor supporting and sustaining software applications maintained by the US Army Human

Resources Command. The contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentiality and security of an individual's PII. The contract specifically states, "HRC is a heterogeneous, enterprise-operating environment consisting of servers, network devices, workstations, printers and other peripherals. Work on this TO may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552A and applicable Army and HRC rules and regulations."

2. Prairie Quest, Inc: The IT contract states - "The contractor shall be responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information which may involve the contractor or the contractor's personnel or to which they may have access may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records maintained by the contractor."

**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.

While being interviewed for Army programs recruiters explain the Privacy Act to individuals and gain the applicant's permission to collect PII. Individuals can object to collection of their PII by choosing to not provide the requested information.

(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.

After a recruiter or other Army representative explains the need for and use of PII collected, and after reading the Privacy Act Statement on the document the individual consents to the specific uses of their PII by signing the document.

(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.

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other                            | <input type="checkbox"/> None                        |

Describe each applicable format.

Several forms are the basis for gathering a person's personally identifiable information electronically and have privacy act statement incorporated into the hard copy. Forms with privacy notification statements include: Record of Military Processing - Armed Forces of the United States (DD Form 1966), Police Record Check (DD Form 369), Privacy Act Statement - Enlisted Recruiting (USAREC Form 1265)(presented to prospect and applicants by US Army Recruiting Command recruiters), Questionnaire for National Security (SF86).

The Secretary of the Army's Partnership for Youth Success (PaYS) program (implemented under AR 601-208) uses a Statement of Understanding for enlisted soldiers and cadets which states "PaYS employers have entered into a Memorandum of Agreement with the US Army and will contact PaYS enlistment applicants during their Army service and during their transition to the civilian sector. PaYS employers are authorized by this SOU to obtain information on PaYS enlistees, including their social security number, home of record, record of military training, home address and phone number, and other information which will facilitate contact with the applicant. PaYS employers are also authorized to release information concerning individual employment status to the Army for purposes of monitoring the success of the program. Information releasable to the Army includes name, social security number, employment status, start date, and generic reasons for employment decisions regarding PaYS applicants."