



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Replacement Operations Automated Management System (ROAMS)

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 3838 (DA00166)
- 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

007-21-01-20-02-2321-00

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

A0600-8-104-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.

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; 42 USC 10606 et seq.; DODD 1030.1, Victim and Witness Assistance; AR 600-8-104, Military Personnel Information Management/Records; AR 600-8-111, DA Pamphlet 600-81; 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 Replacement Operations Automation Management System (ROAMS) provides automated support to the Human Resources Command in its task of projecting filler and casualty replacement requirements and managing filler and replacement flow. ROAMS is an integrated application executed through a series of user-friendly menus, and consists of a corporate database and application software. The ROAMS database is a central repository consisting of two types of data, demographic data from the Integrated Total Army Personnel Data Base (ITAPDB) and ROAMS-unique information. ROAMS contains four modules: the Personnel Flow-Computer Assist Program (FLOWCAP), the Automated Replacement Flow Analysis (AUTOCAP) application, the Automation of the Theater Shelf Requisitioning Process (AUTOREP) application, and a System Security application.

Personal information collected includes personal and military record data.

(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. Staff elements in the chain of command; Department of the Army Inspector General; Army Audit Agency; US Army Criminal Investigation Command; US Army Intelligence and Security Command; Provost Marshall General; and the Assistant Secretary of the Army (Financial Management & Comptroller).

Other DoD Components.

Specify. Office of the Undersecretary of Defense for Personnel and Readiness; Personnel and Readiness Information Management; Defense Finance and Accounting Service; US Air Force; US Marine Corps; US Navy; Defense Intelligence Agency; Joint Services Records Research Center; DOD Inspector General; Defense Manpower Data Center; and Defense Criminal Investigative Service.

Other Federal Agencies.

Specify. National Archives and Records Administration; Department of Veterans Affairs; Office of Personnel Management; Department of Homeland Security; Federal Bureau of Investigation; State Department; Treasury Department;

Department of Labor; Department of Justice; National Reconnaissance Office; Social Security Administration; and Office of the President of the US.

State and Local Agencies.

Specify.

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

Specify. Science Applications International Corporation (SAIC) 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 employee in support of ROAMS 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.

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.

Individuals have the opportunity to object by refusing to provide the requested PII based on the Privacy Act Statement provided at the time enlistment or entrance into military service. However, administrative consequences may ensue if individuals refuse to provide their PII.

(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.

Individuals implicitly consent to specific uses of their time at the time of collection by providing the data.

[Empty light blue box]

(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.

ROAMS verifies existing PII data from other DoD information systems. When data are collected directly from individual Soldiers, they are provided either a Privacy Act Statement or Privacy Advisory.