



PRIVACY IMPACT ASSESSMENT (PIA)

For the

| |
|--|
| Resource Allocation Selection System (RASS) |
| Office of the Assistant G-1 for Civilian Personnel |

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.

5 U.S.C 301, Departmental Regulations; 10 U.S.C 3013, Secretary of the Army, Army Regulation 690-200, General Personnel Provisions; E.O. 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.

RASS is designed to provide a real time, web-based life-cycle management system for centralized management of funds for Army Civilian Training, Education, and Development System ACTEDS-approved DA Intern and Competitive Professional Development (CPD) training. RASS eliminates manual procedures and enables creation, submission, approval, status tracking, and reporting of training request forms. In order to approve and fund training requests, RASS Budget Analysts work in conjunction with the General Fund Enterprise Business System (GFEBS). The URL for RASS is <https://rass.army.mil/index.html>

The RASS operating environment includes a web server, an application server, and a database server. RASS has external links to AKO for CAC/PKI user authentication. RASS also connects internally with the acp02p database residing on APORA02 as required to populate the RASS database with Intern information extracted from the Defense Civilian Personnel Data System (DCPDS). The operating environment is located at the Army Civilian Data Center (ACDC) in Rock Island, Illinois.

The types of PII collected by RASS include personal, educational, and employment information about individuals.

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

Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data thus we believe the risk to the individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection.

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 Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

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.

Information in identifiable form is voluntarily given by the applicant and collected via electronic form on the RASS website.

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

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.

Information in identifiable form is voluntarily given by the applicant and collected via electronic form on the RASS website.

Individuals can refuse to accept the Privacy Act Statement when they access the RASS application.

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

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 type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

| |
|--|
| <p>A Privacy Act statement describing the use, collection and dissemination of personally identifiable information in the system is provided in electronic form upon entering the RASS website.</p> <p>Authority - This information is being collected under the authority of 5 U.S.C. § 4115, a provision of The Government Employees Training Act.</p> <p>Purposes and Uses - The primary purpose of the information collected is for use in the administration of the Federal Training Program (FTP) to document the nomination of trainees and completion of training. Information collected may also be provided to other agencies and to Congress upon request. This information becomes a part of the permanent employment record of participants in training programs, and should be included in the Government wide electronic system, (the Enterprise Human Resource Integration system (EHRI) and is subject to all of the published routine uses of that system of records.</p> <p>Effects and Nondisclosure - Providing the personal information requested is voluntary; however, failure to provide this information may result in ineligibility for participation in training programs or errors in the processing of training you have applied for or completed.</p> <p>Information Regarding Disclosure of your Social Security Number (SSN) Under Public Law 93-579, Section 7(b) - Solicitation of SSNs by the Office of Personnel Management (OPM) is authorized under provisions of the Executive Order 9397, dated November 22, 1943. Your SSN will be used primarily to give you recognition for completing the training and to accumulate Government wide training statistical data and information. SSNs also will be used for the selection of persons to be included in statistical studies of training management matters. The use of SSNs is necessary because of the large number of current Federal employees who have identical names and/or birth dates and whose identities can only be distinguished by their SSNs.</p> |
|--|

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.