



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel System (PNS)

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.

Title 5 US Code Section 301, Departmental Regulations; Title 10 US Code Section 3013, Secretary of the Army; Public Law 107-314; Executive Order 9397 as amended (SSN); Section 636, National Defense Authorization Act; AR 25-1, Army Knowledge Management and Information Technology; and AR 690-200, General Personnel Provisions.

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 Personnel System (PNS) is a client-server application that enables command personnel to track approximately 2,200 users of HRC client-server applications to support business processes associated with security of the applications and tracking of basic personnel information. PNS tracks which applications users can run and the level of security access they have to the system.

The PNS Individual Development Plan (IDP) capability enables all HRC employees to enter their training requests by fiscal year. Managers and training personnel verify data entry, enter costs, approve, and complete training related data. This includes several reports for tracking costs and training for the command in a centralized data store that can be accessed via the LAN. PNS displays training statistics for Soldier Management System training initiatives and computer-based training.

PNS Transfer maintenance allows movement of personnel records from one office to another without re-entry of data. PNS sets up security for different PERMS access levels for SMS, and manages security for all client-server applications by controlling who can do what tasks. Each task is set up using PNS to insert codes for security by individual employee record.

PII collected personal, educational, military, and employment 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.

Staff principals in the chain of command, staff members in Human Resources Command, 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 Department of Defense Inspector General and the Defense Criminal Investigative Service.

Other Federal Agencies.

Specify.

N/A

State and Local Agencies.

Specify.

N/A

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

Specify.

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.

Data are collected directly from HRC staff members (individuals) via direct access to the application, and they have the ability to object and/or question the collection of PII at that time. PNS also retrieves data from information systems rather than directly from individuals, and in those cases individuals are not provided either a Privacy Act Statement or a Privacy Advisory from the system. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

(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.

Data are collected directly from individuals via direct access to the application, and they consent to use of the data by submitting the forms. PNS also retrieves data from information systems rather than directly from individuals, and in those cases individuals are not provided either a Privacy Act Statement or a Privacy Advisory from the system. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

(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.

HRC staff members are provided a Privacy Advisory when they access PNS. Below is the statement that is displayed before accessing the PNS application:
"All information, including personal information, placed on or sent over this system may be monitored."

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.