



PRIVACY IMPACT ASSESSMENT (PIA)

For the

interactive Personnel Electronic Records Management System (iPERMS)

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 USC Section 552a(b)(1), Records maintained on individuals; Title 10 USC Section 3013, Secretary of the Army; Title 44 USC Section 3101, Records management by agency heads, general duties; Title 44 USC Section 3102, Establishment of program of management; EDepartment of Defense Instruction 1336.08, Military Human Resource Records Life Cycle Management; Army Regulation 25-400-2, The Army Records Information Management System (ARIMS); Army Regulation 600-8-104, Army Military Human Resource Records Management; 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 Interactive Personnel Electronic Records Management System (iPERMS) is a highly net-centric system established to provide electronic document management of the Official Military Personnel File (OMPF), and is used to support life-cycle management of Soldiers. iPERMS provides records management in war, mobilization and peace as required by Title 10 US Code (Armed Forces), and Title 44 US Code (Records Management by Federal Agencies). It is the system of record and storage for the OMPF and pay substantiating records during a Soldier's active service; maintains and safeguards the OMPF for 62 years after separation; and then transfers the file to the National Archives for permanent retention. iPERMS is the Army's authorized repository for the OMPF, and is the historical and authoritative source to authenticate a veteran's benefits, entitlements and service. The OMPF is the chronological account of a Soldier's career from accession into the Army through separation, and is a cumulative account of information maintained as evidence of events and decisions during the course of the Soldier's service. The system enhances record quality, optimizes storage and retrieval, reduces operating costs, improves selection board support, and provides numerous other non-quantitative benefits. Soldiers (to include retirees and those deployed to war theaters and other areas of operation), commanders, career managers at all levels, human resource managers, selection boards, and other authorized officials can access iPERMS at all times in a secure mode worldwide. Authorized access to iPERMS is provided to other Federal agencies, such as the Department of Veteran Affairs, the Office of Personnel Management, the Department of Labor, the National Archives and Records Administration, and other outside agencies that require verification of Veteran status and entitlements.

The PII embedded in the digital images of documents in iPERMS includes the following types of information: identification, contact information, military personnel, dependent and family, financial, disability, law enforcement, and education.

(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.

Human Resources managers, Commanders and other Army staff principals in the chain of command, the US Army Reserve Command, the US Army Recruiting 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, the Installation Management Command, and the Assistant Secretary of the Army for Financial Management and Comptroller.

Other DoD Components.

Specify.

The National Guard Bureau, the Office of the Under Secretary of Defense for Personnel and Readiness, Personnel and Readiness Information Management, the Defense Finance and Accounting Service, the Defense Intelligence Agency, the Defense Criminal Investigative Service, the DOD Inspector General, the US Air Force, the US Marine Corps, and the US Navy.

Other Federal Agencies.

Specify.

The National Archives and Records Administration (NARA), the Department of Veterans Affairs, the Office of Personnel Management, the Department of Homeland Security, the Federal Bureau of Investigation, the State Department, the Treasury Department, the Department of Labor, the Department of Justice, the National Reconnaissance Office, the Social Security Administration, and Office of the President of the US.

State and Local Agencies.

Specify.

State and local law enforcement.

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 iPERMS 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.

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.

Each individual has an opportunity to object by refusing to provide the requested PII based on the Privacy Act Statement presented at the time of entrance into military service and in each instance thereafter when PII is solicited by a Human Resource specialist/representative.

(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.

Each individual has an opportunity to object to the specific uses of PII by refusing to provide PII based on the Privacy Act Statement presented at the time of entrance into military service and in each instance thereafter when PII is solicited by a Human Resource specialist/representative.

(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.

A Privacy Act Statement is provided to the individual by a Human Resources Specialist prior to collection of PII data.



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.