



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Military Personnel Office (eMILPO)

Program Executive Office Enterprise Information Systems - Army Human Resource System (PEO EIS ARDS)

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 U.S.C 3013, Secretary of the Army; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 991, Management of deployments of members and measurement and data collection of unit operating and personnel tempo; 10 U.S.C. 482, Quarterly reports: personnel and unit readiness; 10 U.S.C. 165, Combatant commands: administration and support; 10 U.S.C. 166, Combatant commands: budget proposals; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD (P&R)); DoD Instruction 8910.01, Information Collection and Reporting; Chairman of the Joint Chiefs of Staff Manual 3150.13C, Joint Reporting Structure - Personnel Manual; Army Regulation 600-8-23, Standard Installation/Division Personnel System Database Management and E.O. 9397 (SSN), as amended.

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.

Electronic Military Personnel Office (eMILPO) is a web-enabled, multi-tiered, application using an industry standard 2nd generation J2EE platform, implemented on the Department of Defense (DoD) Nonsecure Internet Protocol Router Network (NIPRNet), and accessed via the Army Knowledge Online (AKO) portal. eMILPO provides a reliable, timely, and efficient mechanism for performing personnel actions and strength accounting. Interfacing with 13 essential DoD and Army systems, eMILPO provides Human Capital management to the tactical, theater, and strategic level commander with Title 10 strength management functions. eMILPO standardizes personnel services and management for Active Component (AC) in garrison, all Soldiers on the battlefield and mobilized Reserve Components (RC), providing Multi-Component Unit (MCU) functionality to support Army operations.

eMILPO consolidates the previous AHRs Super Server 43 PPAs database environment into one database. eMILPO's extreme ease of use, providing visibility of location, status, and skills of Soldiers both from a high level and a unit level, is vital in determining the strength and capability for Army commanders. eMILPO serves the active Army during peacetime and all components during mobilization and war.

The use of the data collected is for eMILPO to standardize personnel services and management for Active Component (AC) in Garrison, all Soldiers on the battlefield and mobilized Reserve Components (RC) and provide Multi-Component Unit (MCU) functionality to support Army operations.

The type of PII collected is personal, medical, employment, educational, and military information.

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

Privacy Risks are identified and mitigated by eMILPO system through limited access, Information Assurance compliance, and user training on handling system records. eMILPO access is controlled so only required Army Personnelists and other related staff have limited access to records. Access to records is guarded by physical, administrative and technical controls. Within eMILPO, users are limited to requested functions pertinent to duties relating to personnel services, accounting, Readiness, promotions, and reassignments.

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.

Program Executive Office Enterprise Information Systems (PEO EIS)
Army Human Resources Command (AHRC)
Inspector General (IG)
Department of the Army (DA)
Army Audit Agency (AAA)
Army National Guard Bureau (NGB)

Other DoD Components.

Specify.

N/A

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.

Hewlett Packard (HP) in compliance with AR 25-2 Information Assurance.

Language from Contract: "The Government shall define and maintain security requirements for protecting the system and data. The DTAS SIPR application must have the capability to maintain SECRET data. For all other AHRS applications both the data and systems are sensitive but unclassified. The data must also comply with the U.S. Government Privacy Act Requirements."

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.

Whenever personal information is requested from an individual, they will be furnished a Privacy Act Statement. This Statement is to ensure that individuals know why this information is being collected so they can make an informed decision on whether or not to furnish it.

(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.

The individual will submit a Privacy Act Statement Form for access/amendment, grants, and refusals. The Army is prohibited from disclosing a record from a system of records without obtaining the prior written consent of the data subject.

(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.

As stated in Army Regulation 340-21: Whenever personal information is requested from an individual that will become part of a system of record retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act Statement. This Statement is to ensure that individuals know why this information is being collected. As a minimum, the Privacy Act Statement will include the following information in language that is explicit and easily understood and not so lengthy as to deter an individual from reading it:

(1) Cite the specific statute or Executive order, including a brief title or subject, that authorizes the Army to collect the personal information requested. Inform the individual whether or not a response is mandatory or voluntary and any possible consequences of failing to respond.

(2) Cite the principal purposes for which the information will be used.

(3) Cite the probable routine uses for which the information may be used. This may be a summary of information published in the applicable system notice.

b. The above information normally will be printed on the form used to record the information. In certain instances, it may be printed in a public notice in a conspicuous location such as at check-cashing facilities; however, if the individual requests a copy of its contents, it must be provided.