



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Integrated Military Human Resources System (DIMHRS) - Army

Department of Army/Program Executive Office (PEO) Enterprise Information System (EIS)

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 7972 (AITR #) DA104633
- 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 007-21-01-20-02-0599-00

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 DPR 36 DOD SORN

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. 113 note, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army, Pay and Allowances of the Uniformed Services; 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.

DIMHRS will streamline Army Human Resources (HR), enhancing the efficiency and accuracy of personnel pay procedures. DIMHRS will provide each service member with a single, comprehensive record of service that will feature a self-service capability that allows the Service member to update selected personal information. HR Specialists, Commanders, and others will have access to Soldier personnel and pay information as required to support their decisions and responsibilities across the Army. This web-based HR tool will be available 24 hours a day. PII data collected include military, employment, financial, educational, personal, law-enforcement, medical, biometrics, and beneficiary information.

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

Protection requirements that serve as the foundation for DIMHRS privacy practices are derived from DoDI 8500.2, IA Implementation, and are explicitly defined in the DIMHRS DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (DIP). Awareness and training for all developers and others affected by the privacy plan include local awareness and training, and user consent forms to acknowledge user responsibilities for protecting data. Once implemented, DIMHRS will also have an auditing process to track the actions of any user with access other than self-service. These controls have been incorporated into the DIMHRS DIACAP framework with supporting processes to ensure compliance.

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 Human Resources, All Army Major Commands, the Army Installation Management Command, Army Recruiting Command, Army National Guard Bureau, Army Reserves, and Department of the Army staff, and United States Military Academy

Other DoD Components.

Specify.

Defense Manpower Data Center (DMDC), Defense Finance and Accounting Service (DFAS), United States Air Force, U.S. Navy, U.S. Coast Guard, National Guard Bureau, Defense Manpower Data Center, Office of the DoD Inspector General, Defense Criminal Investigative Service, Office of the Secretary of Defense Personnel and Readiness, Office of the Secretary of Defense

Other Federal Agencies.

Specify.

Department of Veterans Affairs, Office of Personnel Management, Social Security Administration, Department of the Treasury, Department of Homeland Security, Department of Justice

State and Local Agencies.

Specify.

[Empty text box]

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

Specify.

Both the Program Management Support Contractor and the System Development contractor will have access to the system for the purpose of establishing a functional system, but at the point of go-live that access will be revoked. Both contracts will be competed and awarded prior to commencement of system development work. FAR Clause 52.2241-1 Privacy Act Notification and FAR Clause 52.224-2 Privacy Act will be included in these new contracts.

Other (e.g., commercial providers, colleges).

Specify.

Red Cross.

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.

DIMHRS Army will contain the individual's personnel and pay file and all information needed to process related actions. An individual may object to the collection of PII and refuse to provide it. This would, however, preclude any personnel or payroll processing such as a promotion or pay adjustment.

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

[Empty text box]

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.

Army DIMHRS obtains data from AERS and other hire/rehire databases. All individuals requesting entrance into the Army must provide the requisite information in order to gain entrance into the service. An individual may refuse consent to specific uses of PII, however, the PII is required for the personnel and pay processes. Refusal to provide the information will preclude the individual from obtaining the requested service.

--	--

(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 type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

A Privacy Advisory banner will be presented to the individual as they log into the system. In the case of voluntary direct contact by the User with the HR Specialist, no security information is provided.

--	--

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.