



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Enrollment Eligibility Reporting System (DEERS)

Defense Manpower Data Center

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

0704-0415

Enter Expiration Date

31 Dec 2010

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. Chapters 53, Miscellaneous Right and Benefits, Chapter 54, Commissary and Exchange Benefits, Chapter 55 Medical and Dental Care, Chapter 58 Benefits and Services for Members being Separated or Recently Separated, and Chapter 75 Deceased Personnel; 10 U.S.C. 136 Under Secretary of Defense for Personnel Readiness; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S.C. 3512(c) Executive Agency Accounting and Other Financial Management; 50 U.S.C. Chapter 23, Internal Security; DoD Directive 1341.1, Defense Enrollment/ Eligibility Reporting System; DoD Instruction 1341.2, DEERS Procedures; 5 U.S.C. App. 3 (Pub.L. 95-452, as amended Inspector General Act of 1978; Pub.L. 106-265, Federal Long-Term Care Insurance; and 10 U.S.C. 2358, Research and Development Projects; 42 U.S.C., Chapter 20, Subchapter I-G, Registration and Voting by Absent Uniformed Services Voters and Overseas Voters in Elections for Federal Office, Sec. 1973ff, Federal responsibilities and DoD Directive 1000.4, Federal Voting Assistance Program (FVAP); Homeland Security Presidential Directive 12, Policy for a common Identification Standard for Federal Employees and Contractors; 38 CFR part 9.20, Traumatic injury protection, Servicemembers' Group Life Insurance and Veterans' Group Life Insurance; and E.O. 9397 (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 purpose of the system is to provide a database for determining eligibility to DoD entitlements and privileges; to support DoD health care management programs; to provide identification of deceased members; to record the issuance of DoD badges and identification cards, i.e. Common Access Cards (CAC) or beneficiary cards; and to detect fraud and abuse of the benefit programs by claimants and providers to include appropriate collection actions arising out of any debts incurred as a consequence of such programs.

To authenticate and identify DoD affiliated personnel (e.g., contractors); to assess manpower, support personnel and readiness functions; to perform statistical analyses; identify current DoD civilian and military personnel for purposes of detecting fraud and abuse of benefit programs; to register current DoD civilian and military personnel and their authorized dependents for purposes of obtaining medical examination, treatment or other benefits to which they are entitled; to ensure benefit eligibility is retained after separation from the military; information will be used by agency officials and employees, or authorized contractors, and other DoD Components for personnel and manpower studies; and to assist in recruiting prior-service personnel.

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

The privacy risks associated with the collection of PII are low. The security features of DEERS provide a level of protection that meets or exceeds the minimal requirements of DoD Directive 8500.2. The concept of identification and authentication "layered protection" is used to keep unauthorized users out of the DEERS PDR. All personnel granted access must participate in a security training and awareness program. This program consists of both initial security training and annual refresher training.

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.

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.

Disclosure is printed on DD Forms 1172, 1172-2 and 2842: Voluntary; however, failure to provide information may result in denial of a Common Access Card; non-enrollment in DEERS; refusal to grant access to DoD installations, buildings, facilities, computer systems and networks; and denial of DoD benefits and privileges if authorized.

(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.

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

The DEERS System of Records Notice provides the purpose of collection and the routine uses (i.e. providing benefits), but the individuals consent was provided at the time of collection.

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.

Privacy Act Statements are printed on DD Forms 1172, 1172-2 and 2842 and provided at the collection point. The statement provides collection purpose, authorities; external uses, nature of the program, the name and number of the PAS notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. A PAS is also available for those updating their information via telephone.

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.