DEFENSE MANPOWER DATA CENTER (DMDC)

PRIVACY IMPACT ASSESSMENT (PIA)
for the
DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM (DEERS)

15 December 2006

Prepared By: Pam R. Bridges
DEERS Project Officer

Introduction

The E-Government Act of 2002 (Public Law 107-347,44 U.S.C., CH 46) requires all Federal government agencies to conduct Privacy Impact Assessments (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information.

The Office of Management and Budget (OMB) Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (dated 26 Sep 03), Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance Memorandum on Publishing Impact Assessments provides information to agencies and the DoD on Implementing the provisions.

E-Government Act Section 208 Implementation Guidance

A PIA is a process for determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form.

The E-Government Act requires that agencies conduct a PIA before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form or (ii) initiating a new electronic collection of information that will be collected from ten or more persons, other than agencies, instrumentalities, or employees of the Federal Government, and will be maintained, or disseminated in an identifiable form, using information technology.

PIAs are conducted to ensure that there is no collection, storage, access, use, or dissemination of identifiable information from or about members of the general public and businesses that is not needed or authorized, and that identifiable information that is collected is adequately protected. PIAs may address issues relating to the integrity and availability of data handled by a system, to the extent these issues are not already adequately addressed in a System Security Plan.

Definitions:

Information in identifiable form: Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Information technology (IT): As defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

DEERS PRIVACY IMPACT ASSESSMENT (PIA)

1. **Department of Defense (DoD) Component**: Defense Manpower Data Center (DMDC)

2. **Name of Information Technology (IT) System**: Defense Enrollment/Eligibility Reporting System (DEERS)

3. **Budget System Identification Number (SNAP-IT Initiative Number):** 4035

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):** 1391

5. **IT Investment (OMB Circular A-11) Unique Identifier (if applicable):** 007-97-01-15-01-4035-00-403-254

6. **Privacy Act System of Records Notice Identifier**: S322.50 (Defense Eligibility Records (May 11, 2004), 69 FR 26081)

7. **OMB Information Collection Requirement Number (if applicable) and Expiration Date:** N/A

8. **Type of authority to collect information**: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. Chapters 53,54,55,58 and 75; 10 U.S.C. 136; 31 U.S.C. 3512©; 50 U.S.C. Chapter 23, Internal Security; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 1341.2, DEERS Procedures; Homeland Security Presidential Directive (HSPD)-12; 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 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); 38 CFR part 9.20, Traumatic Injury Protection, Servicemembers' Group Life Insurance and Veterans' Group Life Insurance; and E.O. 9397 (SSN).

9. **Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):** The Defense Enrollment Eligibility Reporting System (DEERS) is a centralized Person Data Repository (PDR) designed to provide timely and accurate information on those eligible for DoD benefits and entitlements.DEERS collects and maintains information to ensure and facilitate the effective and efficient administration of DoD missions to include the military health system and other benefit and entitlement programs that derive eligibility information from the PDR.The PDR database contains detailed personnel eligibility information for benefits and entitlements to Uniformed Service members; foreign military members;

Uniformed Service civilians and contractors and other personnel as directed by DoD and their eligible family members. DEERS data is used to authenticate the Real-Time Automated Personnel Identification System (RAPIDS). The Common Access Card (CAC) and/or DEERS enrollment control access to and movement in or on DoD Installations, buildings, or facilities; regulate access to DoD computer systems and networks; and verify eligibility, if authorized, for DoD benefits and privileges.DEERS also authenticates identity for security purposes. The Defense Eligibility Enrollment Reporting System (DEERS) uses a layered approach to data access, preparation, and transformation. Modular units, composed of common and re-usable components arranged in layers by function, contain the software code and the rules or knowledge with which to process this data. These units are grouped into a hierarchy of control and abstraction. Discrete, narrow interfaces between units enforce encapsulation, hide information from unauthorized users, and provide the opportunity for expanding data processing capabilities and functionality in a modular way.

- **System Administration Office**: DMDC, 1600 Wilson Blvd, Suite 400, Arlington, VA 22206
- **System Administration (Backup) Office**: DOD Center Monterey Bay, DMDC, 400 Gigling Road, Seaside, CA 93955
- **System Owner**: Deputy Director, DMDC, 400 Gigling Road, Seaside, CA 93955

10. **Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, social security numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.):** Identifiable data elements collected (public only): Name, gender, race, social security number, organization, citizenship, date of birth, place of birth, residence address, supplemental address, office e-mail & alternate e-mail address. Nature and source of data identified in item 11.

11. **Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc):** DEERS' PDR is updated by batch transactions from the Uniformed Services' automated personnel, finance, medical and mobilization management systems, the Department of Veterans Affairs (VA), and the Centers for Medicare and Medicaid Services (CMS). DEERS is also accessed and updated by online DEERS Client applications, such as the Real-Time Automated Personnel Identification System (RAPIDS), Contractor Verification System (CVS) and interfacing client systems of the Military Health System (MHS), such as the Composite Health Care System (CHCS). Information is also collected by the individual completing DD Forms 1172,1172-2, and 2842.

12. **Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.):** To provide DEERS enrollment and eligibility for DoD benefits and privileges; to provide verification for issuance of DoD authorized identification cards or Common Access Card (CAC) - used to control access to and movement in or on DoD Installations, buildings, or facilities and to regulate access to DoD computer systems and networks.

    Homeland Security Presidential Directive (HSPD)-12 requires that a common card be developed for identification of Federal employees. The DoD Common Access Card (CAC) has been expanded to meet the requirements of HSPD-12.

    DoDD 1000.25 – 4. Policy, 4.1 Issuance of DoD identity credentials shall be accomplished using authentication of identity. RAPIDS is used to issue the definitive credential of affiliation with the DoD. It relies on the information stored in the DEERS PDR. Once issued, the DoD credential shall serve as the definitive assertion of identity and shall be authenticated against the DEERS PDR, global directory services, or DoD PKI services in real time whenever possible. 4.1.1 Authenticate individuals to ensure that DoD identification credentials are provided only to those with a current and appropriate affiliation with the Department of Defense. 4.1.3 Provide a distinct identification credential for use as proof of identity and DoD affiliation and may act as the Geneva Conventions Card in accordance with DoDI 1000.13 and as an authorization card for Uniformed Services' benefits and privileges.

    DoDI 1000.13 – 4. Policy …to provide members of the Uniformed Services with a distinct ID card for use in identifying their status as active duty, Reserve, or retired members and as an authorization card for Uniformed Services' benefits.

    DoDI 1341.2 – 4. Policy, 4.1. The scope of DEERS shall include the capability of DEERS to: 4.1.2 Provide information for generating Uniformed Services' sponsor and family member identification (ID) cards.

13. **Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.):** To authenticate and identify DoD affiliated personnel; 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 the purposes of obtaining medical benefits or other benefits for which they are qualified; to ensure benefit eligibility is retained after separation; for manpower and personnel studies and to assist in recruiting prior-service personnel.

14. **Describe whether the system derives or creates new data about individuals through aggregation:** No.

15. **Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.):** To Federal and State agencies and private entities, as necessary, on

matters relating to utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government and contractor facilities, computer systems, networks and controlled areas.

16. **Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent:** 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.

17. **Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form:** Privacy Act Statements, as required by 5 U.S.C. 552a(e)(3), are printed on DD Forms 1172, 1172-2 and 2842 and provided at the collection point. The statement provides the following: collection purpose, authorities, external uses, nature of the program, the name and number of the Privacy Act System notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms.

18. **Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect and preserve the confidentiality of the information in identifiable form:** Computerized records are maintained in a controlled area accessible only to authorized personnel. Entry to these areas is restricted to those personnel with a valid requirement and authorization to enter. Physical entry is restricted by the use of locks, guards and administrative procedures. All personnel who access DEERS data are required to have a public trust rating of Information Technology (IT)-I or IT-II depending on job role. Access to personal information is restricted to those who require the records in the performance of their official duties and to the individuals who are the subjects of the record or their authorized representatives. Access to personal information is further restricted by use of CAC or passwords which are changed periodically. All individuals responsible for system maintenance receive initial and periodic refresher Privacy Act and Security training. Users are warned through log-on procedures of the conditions associated with access and the consequences of improper activities.Users are trained to lock workstations when leaving them unattended and to shut down computers when leaving at the end of the day. Workstations are automatically locked after ten minutes of inactivity. The DMDC infrastructure, within which DEERS is housed and controlled, conforms to full DITSCAP / DIACAP as reflected in DoD regulations, including, but not limited to: DoDD 5200.2, DoDI 8500.2, and is covered by a current AtO (Authority to Operate).

19. **Identify whether the IT system or collection of information will require a System of Records notice defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program, "November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the notice will occur:** Yes. System of Records Identifier listed in question 6.

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:** 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.

    THREATS: Access, storage and transmission of information protected under the Privacy Act of 1974 are subject to threats, including, but not limited to: malware, sniffing, spoofing, and physical assault, as well as various natural disasters and failures which impact either the protected infrastructure or the services upon which the infrastructure depends. All of these imperil, to one extent or another, information availability, integrity, and confidentiality.

    DANGERS: There are no known dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at time of data collection via a Privacy Act Statement. Individuals are free to raise objections if new threats are perceived.

RISKS	MITIGATION	ASSESSMENT
		(HIGH) (MED) (LOW)
Userid/password/CAC used by someone other than whom assigned	Allocation of passwords is managed and password security policies enforced. There is the possibility of loss of PII data on an individual basis.	(MED)
Mishandling of sensitive data, reports, or storage media	Periodic assessments of access rights and privileges are performed	(LOW)
Virus attacks and other malicious incidents	System controls are predicated on preventing unauthorized users from accessing DEERS resources.	(LOW)
Loss of CAC	It is the responsibility of the CAC holder to use certificates and private keys for official use only; protect private key from unauthorized use; report loss or compromise to RAPIDS issuing facility. With the loss of a CAC, one would have to also know the pin to use the CAC. Even if an attempt was made to guess the PIN, if there are three wrong guesses, the card will lock out all access. There is the possibility of loss of PII data on an individual basis.	(MED)

21. **State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form**. Accreditation permits data to be processed as sensitive unclassified and is protected by the Privacy Act of 1974 in the system high mode of operation, as defined in DoD Directive 5200.40. PIA should be published in full.

Preparing Official Pam R. Bridges (14 DEC 06) **(signature) (date)**

Name: Pam R. Bridges
Title: DEERS Project Officer
Organization: Defense Manpower Data Center
Work Phone: (831) 583-4044
Email: **pamela.bridges@osd.pentagon.mil**

Information Assurance Official _____ **(signature) (date)**

Name: Victoria Galante
Title: Information Assurance Officer
Organization: Defense Manpower Data Center
Work Phone: (831) 583-5447
Email: victoria.galante@osd.pentagon.mil

Privacy Officer William Boggess **(signature) (date)**

Name: William Boggess
Title: Chief Information Officer
Organization: Defense Manpower Data Center
Work Phone: (831) 583-4170
Email: william.boggess@osd.pentagon.mil

Reviewing Official Mary Snavely-Dixon 18 Dec 2006 **(signature) (date)**

Name: Mary Snavely-Dixon
Title: Director
Organization: Defense Manpower Data Center
Work Phone: (703) 696-7423
Email: mary.dixon@osd.pentagon.mil