PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Enrollment Eligibility Reporting System (DEERS)

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

02/22/19

Defense Manpower Data Center (DMDC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To manage the issuance of DoD badges and identification cards, i.e., Common Access Cards (CAC) or beneficiary identification cards.

To authenticate and identify DoD affiliated personnel (e.g., contractors); to manage physical and logical access to DoD facilities.

To provide a database for determining eligibility for DoD entitlements and privileges; 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 identify current DoD civilian and military personnel for purposes of detecting fraud and abuse of benefit programs; to ensure benefit eligibility is retained after separation from the military; to maintain the Servicemembers' Group Life Insurance (SGLI) and Family SGLI (FSGLI) coverage elections and beneficiaries' information.

To support DoD health care management programs, to include research and analytical projects, through Defense Health Agency (previously the TRICARE Management Activity); to support benefit administration for those beneficiaries that have granted permission for use of their personal email address for notification purposes relating to their benefits; 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 provide identification of deceased members.

To assess manpower, support personnel and readiness functions, to include Continuous Evaluation programs; to perform statistical analyses; to determine Servicemembers Civil Relief Act (SCRA) duty status as it pertains to SCRA legislation; to determine Military Lending Act (MLA) eligibility as it pertains to MLA legislation; information will be used by agency officials and employees, or authorized contractors, and other DoD Components in the preparation of studies and policy as related to manpower and the health and well-being of current and past Armed Forces and DoD-affiliated personnel; to assist in the Transition Assistance Program (TAP); to assist in recruiting prior-service personnel; and to notify military members eligible to vote about information for registration and voting procedures; and to provide rosters of DoD affiliated persons at the time of an official declared natural or man-made disaster.

To provide appropriate contact information of DoD personnel and beneficiaries for the purpose of conducting surveys authorized by the Department of Defense. Authorized surveys are used as a management tool for statistical analysis, policy planning, reporting, evaluation of program effectiveness, conducting research, to provide direct feedback on key strategic indicators, and for other policy planning purposes

The types of personal information collected in this system include Name, Social Security Number (SSN), DoD ID Number, personal and work contact information, date of birth, gender, emergency contact information, and biometric information. For a complete list of elements, see Section 2(a).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected in order to authenticate and identify DoD affiliated personnel; provide enrollment and eligibility information for DoD benefits and privileges; and provide verification for issuance of DoD authorized identification or common access cards. Additionally, information is used for Computer Matching purpose as authorized in accordance with the Privacy Act of 1974.

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

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

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

Individuals provide consent at the point of collection.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	Various OSD Offices
[X] Other DoD Components	Specify.	Each of the Uniformed Services
[X] Other Federal Agencies	Specify.	Transportation Security Administration; Social Security Administration; Department of Veterans Affairs; OPM; United States Postal Service; Executive Office of the President and Administrative Office of the Courts; Department of Health and Human Services; Department of Education; Department of Labor; Coast Guard; Public Health Service; American Red Cross; Department of Homeland Security.
[X] State and Local Agencies	Specify.	State Medicaid agencies; Consumer Reporting Agencies.
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Contracted Medical Health providers; Defense contractors.
[X] Other *(e.g., commercial providers, colleges)*.	Specify.	Pharmacies; Federally Funded Research Centers.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[ ] Databases
[X] Existing DoD Information Systems
[ ] Commercial Systems
[X] Other Federal Information Systems

DoD Personnel, Pay and Benefit systems; Department of Veterans Affairs and other Federal agencies.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [x] Telephone Interview
- [x] Information Sharing - System to System
- [x] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

DD Forms 1172, 1172-2 and 2842

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier DMDC 02

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-330-03-001

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Hardcopy version of DD Form 1172: Destroy once written to optical disk. Optical disks: Destroy primary and backup copies after 5 years. The DEERS database is Permanent: Cut off (take a snapshot) at end of Fiscal Year and transfer to the National Archives and Record Administration in accordance with 36 CFR 1228.270 and 36 CFR 1234. (N1-330-03-01) Output records (electronic or paper summary reports) are deleted or destroyed when no longer needed for operational purposes. Note: This disposition instruction applies only to record keeping copies of the reports retained by DMDC. The DoD office requiring creation of the report should maintain its record keeping copy in accordance with NARA guidelines.

m. What is the authority to collect information? A Federal Law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Federal Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 10 U.S.C. 987, Terms of Consumer Credit Extended to Members and Dependents; 20 U.S.C. 1070h, Scholarships for Veteran's Dependents; 31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management Reports and Plan; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); 42 U.S.C. 1973ff, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; 50 U.S.C. Chapter 50, Servicemembers Civil Relief Act; DoD Directive 1000.04, Federal Voting Assistance Program (FVAP); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP)

Program; DoD Instruction 1015.9, Professional United States Scouting Organization Operations at United States Military Installations Located Overseas; DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Instruction 1241.03 TRICARE Retired Reserve (TRS) Program; DoD Instruction 1241.04, TRICARE Reserve Select (TRS) Program; DoD Instruction 1336.05, Automated Extract of Active Duty Military Personnel Records; DoD Instruction 1341.2, DEERS Procedures; DoD Manual 1341.02, DoD Identity Management DoD Self-Service (DS) Logon Program and Credential; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; DoD Instruction 7730.54, Reserve Components Common Personnel Data System (RCCPDS); 38 CFR 9.20, Traumatic injury protection; 38 U.S.C. Chapter 19, Subchapter III, Service members' Group Life Insurance; and E.O. 9397 (SSN), as amended

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB#: 0704-0415
Expiration Date: 3/31/2020

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[X] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[ ] Driver's License	[X] Education Information	[X] Emergency Contact
[X] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[ ] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[ ] Medical Information
[X] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[ ] Passport Information	[X] Personal E-mail Address	[X] Photo
[X] Place of Birth	[X] Position/Title	[ ] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[ ] Records	[X] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[ ] If Other, enter the information in the box below	

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Approved 30 August 2018

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Acceptable uses 2, Law Enforcement, National Security and Credentialing; 8, Computer Matching; 13, Other cases (to assist other components in complying with DoDI 1000.30).

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

This system utilized the DoD ID when possible. The SSN is afforded the highest protections practicable through appropriate administrative, technical and physical safeguards.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [X] No

The SSN is a requirement for CAC issuance and governance of the DoD ID number.

b. What is the PII confidentiality impact level[2]? [ ] Low [X] Moderate [ ] High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [x] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [ ] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [x] Encryption of Data in Transit
- [ ] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [x] Least Privilege Access
- [ ] User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?