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 Manpower Data Center Data Base

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

04/14/21

Defense Manpower Data Center

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.

The purpose of this system of records is to provide a single repository within the Department of Defense to assess manpower and pay trends, support personnel and readiness functions, track deployments, assist recruiting efforts, locate and fill vacant positions, track career progression from applicant/accession to separation, to perform longitudinal statistical analyses, identify current and former DOD civilian and Armed Forces personnel for purposes of detecting fraud and abuse of pay and benefit programs, to register current and former DOD civilian and Armed Forces personnel and their authorized dependents for purposes of obtaining medical examination, treatment, privileges , or other benefits to which they are qualified.

To collect debts owed to the United States Government and state and local governments.

Information will be used by agency officials and employees, or authorized contractors, and
other DOD Components in the preparation of surveys, research, and policy as related to the health and well-being of current and past Armed Forces and DOD affiliated personnel; to respond to Congressional and Executive branch inquiries; and to provide data or documentation relevant to the testing or exposure of individuals.

Military Services and Civilian drug test records will be maintained and used to conduct longitudinal, statistical, and analytical studies and computing demographic reports. No personal identifiers will be included in the demographic data reports. All requests for Service specific drug testing demographic data will be approved by the Service designated drug testing program office. All requests for DoD wide drug testing demographic data will be approved by the DoD Director for Drug Testing and Program Policy, 4000 Defense Pentagon, Washington, DC 20301-4000. Drug data will also be used to support the continuous evaluation program for personnel security vetting and monitoring for personnel being evaluated for access to national security information. Former service drug test records and Civilian drug records are precluded from use for continuous evaluation programs.

DMDC web usage data will be used to validate continued need for user access to DMDC computer systems and databases, to address problems associated with web access, and to ensure that access is only for official purposes.

Types of personal information collected include: name, social security number, DoD Identification Number, date of birth, selective service number, civil service claim number, rank, age, sex, race, education, home town, home address, work address, hospitalization, casualty information, medical treatment, fingerprints, credit or financial data, agency identifier, metropolitan statistical area, e-mail address, phone number.

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)*

Personally Identifiable Information is collected and maintained for data matching and mission-related uses. Information within these files are used to meet the Department's readiness requirements as well as to conduct research and studies relating to the health and well-being of past and present DoD affiliated personnel.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ 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.

PII is provided to DMDC 01 by other systems . Most of the files contained in this System are from DoD Pay and Personnel files. For these individuals a Privacy Act Statement is provided during initial entry into Service on the Service specific personnel forms (e.g. DA form 61, NAVMC 763, USAFA Form 146 and AETC Forms 1413 & 1422). For the Armed Services Vocational Aptitude Battery (ASVAB) and Defense Language Proficiency Test (DLPT) files individuals can elect not to take the test.

f. 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.

For all other files contained in the DMDC 01 System contains PII provided by other systems. Note: For Military personnel- A Privacy Act Statement is provided during initial entry into Service on the following Service specific personnel forms (e.g. DA form 61, NAVMC 763, USAFA Form 146 and AETC Forms 1413 & 1422). On these forms individuals agree to the collection of their data for military personnel uses, but do not agree to all specific uses ie. data matching, surveys, statistical compilations etc.

For the ASVAB files: individuals taking the ASVAB test are provided the following statement, “Privacy Act Statement Authority: Sections 505, 508, 510, and 3012 of Title 10
U.S. Code and Executive Order 9397. PRINCIPAL PURPOSE: the requested information on this form will be used to properly process and identify the individual requesting an examination at a military entrance processing station (MEPS). ROUTINE USE: Record is maintained with other enlistment processing records. DISCLOSURE: Voluntary: refusal to provide required data could result in denial of enlistment.

For the DLPT Database: individuals taking the DLPT test are provided a privacy act statement.

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.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

DMDC does not solicit information directly from the individuals.

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

☒	Within the DoD Component	Specify.	each of the Services
☒	Other DoD Components	Specify.	DFAS
☒	Other Federal Agencies	Specify.	Department of Veteran Affairs, Office of Personnel Management, Internal Revenue Service, Health and Human Services, Social Security Administration, Homeland Security, Department of Education
☒	State and Local Agencies	Specify.	State Veteran Affairs office, State and Local Law Enforcement
☐	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.	
☒	Other *(e.g., commercial providers, colleges)*.	Specify.	Federally Funded Research and Development Centers (FFRDCs)

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

- [ ] Individuals
- [ ] Databases
- [x] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

Service Personnel Systems, Department of Veteran Affairs, Office of Personnel Management, Health and Human Services, Department of Energy, Executive Office of the President, Selective Service System

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

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

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 01

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 item4b(2)

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

(3) Retention Instructions.

The retention is Permanent. At the end of each fiscal year, a snapshot of the Master File together with the system documentation are transferred to the National Archives and Records Administration in accordance with 36 CFR part 1228.270 and 36 CFR part 1234.

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 (Pub.L. 95-452, as amended (Inspector General Act of 1978)); National Defense Authorization Act (NDAA) Fiscal Year 2020 , DoD Instruction 6490.03, Deployment Health; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1562, Database on Domestic Violence Incidents; 20 U.S.C. 1070(f)(4), Higher Education Opportunity Act; Pub.L. 106-265, Federal Long-Term Care Insurance; 10 U.S.C. 2358, Research and Development Projects; 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.

☐ 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.

Information is not collected directly from the individual, rather from other Federal source systems.

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	[ ] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[ ] Driver's License	[X] Education Information	[ ] Emergency Contact
[X] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[ ] Home/Cell Phone	[ ] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[ ] Marital Status	[ ] Medical Information
[X] Military Records	[ ] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[ ] Other ID Number
[ ] Passport Information	[ ] Personal E-mail Address	[ ] Photo
[ ] Place of Birth	[X] Position/Title	[X] Protected Health Information (PHI)[1]
[ ] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[ ] Records	[ ] 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.

Lyn Kirby, Chief, DPCLTD. February 24, 2021.

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

Acceptable uses (8) "Computer Matching" and (11) "Legacy System Interface"

(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".

The SSN is used for Computer Matching purposes between DoD and other Federal agencies that continue to use the SSN as a primary identifier. Additionally, the DMDC Data Base receives records from each of the Service's personnel systems. Currently, several of the Service personnel systems have yet to transitioned to the DoD ID Number. The only way to uniquely identify using the above named data source is to request and use the SSN. Wherever possible, the DoD ID is used in lieu of the SSN.

(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

This system interacts with DoD legacy systems that have not fully transitioned to the DoD ID. Additionally, this system interacts with other Federal agencies that do not use the DoD ID. Internally, the preferred identifier is DoD ID.

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

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

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

Access to personally identifiable information is restricted to those individuals who require access to the records in the performance of their official duties. Access to personally identifiable information is further restricted by the use of Personal Identity Verification (PIV) cards and PIN. Physical entry is restricted by the use of locks, key cards, security guards, and identification badges. All individuals granted access to this system of records will have completed annual Information Assurance and Privacy Act training and be appropriately vetted. Audit logs will be maintained to document access to data. All electronic data transfers into this system of records will be encrypted. Records will be maintained in a secure database with an intrusion detection system in a physically controlled area accessible only to authorized personnel.