PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Manpower Data Center Data Base (DMDC 01)
Department Defense Manpower Data Center (DMDC)

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** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

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 1391

☐ **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 007-97-01-15-01-4035-00

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 DMDC 01

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. TBD

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 O7O4-O536

Enter Expiration Date O6/3O/2O15

☐ **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. App. 3 (Pub. L. 95-452, as amended (Inspector General Act of 1978)); 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. 1070a(f)(4), Higher Education Opportunity Act, Public Law 106-265, Federal Long-Term Care Insurance; 10 U.S.C. 2358, Research and Development Projects; 5 U.S.C. 2108a, Veterans Opportunity to Work (VOW) to Hire Heroes Act of 2011, Public Law 112-56; and E.O. 9397 (SSN), as amended.

DoD Instruction 1215.07, DoD Instruction 1336.05, DoD Instruction 1444.02 (Vol 1, 2, 3, &4), DoD Instruction 6490.03, DoD Instruction 5000.55, DoD Reorganization Act of 1986 (Title IV), National Defense Authorization Act (NDAA) for FY 2000/2001, DoD 6400.1-M-1, DoD Instruction 7730 .54, DoD Instruction 7730 .64, Public Law 102-4, Agent Orange Act of
1991, National Defense Authorization Act for Fiscal Year 1994 , Title 10, Section 1153, DoD Instruction 7770 .01, DoD Instruction 7770 .02, DoD Instruction 7770.03, DoD Instruction 1300 .18, DoD Instruction 5160 .70, DoD Instruction 1336 .1, DoD Instruction 1336 .07, DoD Instruction 1010 .01, FY91 National Defense Authorization Act (Section 1143(a) of Public Law 101-510), Improper Payments Elimination and Recovery Improvement Act (IPERIA).

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 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, medical treatment, fingerprints, credit or financial data, agency identifier, metropolitan statistical area, e-mail address, phone number.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion, hacking and data leakage due to a careless employee. There are risks that the Defense Manpower Data Center Data Base, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls are put in place on the DMDC 01 system as listed below.

The following controls are used to mitigate the risks:

Physical entry to the facility is restricted by the use of fences, gates, locks, federal police, guards, closed circuit TV, and administrative procedures. 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. All personnel who access DMDC 01 data are required to have a public trust (or interim 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 records or their authorized representatives.

Access to personal information is further restricted by use of CAC. All individuals responsible for system maintenance receive initial and periodic refresher Privacy Act and Information Assurance 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.

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.

Office of the Secretary of Defense
Joint Staff
Combatant Commands
Office of the Inspector General
Defense Agencies
DoD Field Activities

☒ **Other DoD Components.**

Specify.

Department of Air Force
Department of Army
Department of Navy
(to include agencies established therein)

☒ **Other Federal Agencies.**

Specify.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S. C. 552a(b)(3)

Department of Veteran Affairs
Office of Personnel Management
Internal Revenue Service
Department of Health and Human Services
Social Security Administration
Department of Labor
Department of Homeland Security
Department of State
Department of Interior
Department of Treasury
Department of Justice
United States Postal Service Government Accountability Office
National Oceanic and Atmospheric Administration
Public Health Service
United States Coast Guard
National Archives and Records Administration (NARA)
Census Bureau

Centers for Disease Control
Selective Service

☒ **State and Local Agencies.**

In support of Federal reporting requirements, or at the permission of the individual about whom the record pertains:

Specify. State of Alaska-Department of Revenue
New Mexico Taxation and Revenue Department
State VA Agencies

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

Specify. Defense contractors. Contracts include required language by the FAR for safeguarding PII.

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

Specify. Federally Funded Research Development Centers (FFRDC)

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.

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

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.

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.

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.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

DMDC 01 does not supply Privacy Act Statements since the system does not collect data directly from the individual. However, individuals whose records appear in DMDC 01 should have been provided a Privacy Act Statement upon providing their data to personnel, pay, or other DMDC 01 data sources.

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.