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:

MIRS 1.1 - MEPCOM Integrated Resource System 1.1

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

United States Military Entrance Processing Command (USMEPCOM)

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] 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.

MIRS provides the automation and communications capability for USMEPCOM to meet its peacetime, mobilization, and wartime military manpower accession mission for the Armed Services.

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)*

To establish eligibility for enlistment (identification and authentication), verify enlistment and placement scores, verify retest eligibility, and provide aptitude test scores as an element of career guidance to participants in the Department of Defense (DoD) Student Testing Program. The data is also used for research, marketing evaluation, assessment of manpower trends and characteristics, and related statistical studies and reports.
Mission-related - USMEPCOM is currently the only DoD organization legally authorized to collect, civilian, medical and testing data for purposes of processing enlistment applicants into the military. USMRIS is the only DoD Joint support system in operation that is used to enforce congressional, DoD and Armed Forces qualifications. criteria for enlistment. It is used as an official system for reporting timely enlistment accession data to DMDC. Information collected is also disclosed to the Selective Service Systems (SSS) to update its registrant database and may also be disclosed to local and state Government agencies for compliance with laws and regulations governing control of communicable diseases.

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.

Personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement.

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

All collected information is required for applicant processing into one of the Armed Services.

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

All forms requesting PII data have an applicable Privacy Act Statement.

PRIVACY ACT STATEMENT - HEALTH CARE RECORDS

THIS FORM IS NOT A CONSENT FORM TO RELEASE OR USE HEALTH CARE INFORMATION PERTAINING TO YOU.
AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN)
Sections 133, 1071-87, 3012, 5031 and 8012, title 10, United States Code and Executive Order 9397.
PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED
This form provides you the advice required by the Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.

ROUTINE USES
The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to:
Aid in preventive health and communicable disease control programs
and report medical conditions required by law to federal, state and local
agencies;
compile statistical data;
conduct research;
teach;
determine suitability of persons for service or assignments;
adjudicate claims and determine benefits;
other lawful purposes, including law enforcement and litigation;
conduct authorized investigations;
evaluate care rendered;
determine professional certification and hospital accreditation;
provide physical qualifications of patients to agencies of federal, state, or local
government upon request in the pursuit of their official duties.

WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION

In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED.

This all inclusive Privacy Act Statement will apply to all requests for personal information made by health care treatment personnel or for medical/dental treatment purposes and will become a permanent part of your health care record.

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

☒ Within the DoD Component	Specify.	Army Recruiting Information Support System (ARISS), Army Research Institute (ARI), United States Army Recruiting Command (USAREC), United States Army Accessions Command (USAAC), United States Army Cadet Command (USACC), United States Training and Doctrine Command (TRADOC), United States Army Deputy Chief of Staff for Personnel (G-1), Army Medical Surveillance Activity (AMSA) - USACHPPM, U.S. Army Medical Command (MEDCOM)
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Air Force Reserve Command (AFRC), Air Force Recruiting Information Support System (AFRISS), Marine Recruiting Information Support System (MCRISS), Navy Drub Screening Lab (NDSL), Navy Recruiting Accession Management System (NRAMS)

☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Marine Corps Recruiting Information Support System (MCRISS), Marine Corps Recruiting Command (USMCRC), Naval Education and Training, Professional Development and Technology Center (NETPDTC), Navy Drug Screening Lab, Navy Recruiting Accession Management System (NRAMS), Space and Naval Warfare - Information Technology Center (SPAWAR-ITC), US Navy Recruiting Command (NRC), Air Force Reserve Command, Air Force Recruiting Information Support Systems (AFRISS), Defense Finance and Accounting Service, Defense Integrated Military Human Resource Command (DIMHRS), Defense Manpower Data Center, Defense Security Service (DSS), Military Surface Deployment and Distribution Command (SDDC), Accession Policy (AP), Military Personnel Policy (MPP), Personnel and Readiness (P&R), Department of Defense Medical Examination Review Board (DoDMERB), Office of the Surgeon General
☒ State and Local Agencies	Specify.	Army Reserve National Guard
☐ 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.	

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

- ☒ Individuals
- ☒ Existing DoD Information Systems
- ☒ Other Federal Information Systems
- ☒ Databases
- ☐ Commercial Systems

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

- ☐ E-mail
- ☒ In-Person Contact
- ☐ Fax
- ☒ Information Sharing - System to System
- ☐ Other *(If Other, enter the information in the box below)*
- ☒ Official Form (*Enter Form Number(s) in the box below)*
- ☐ Paper
- ☐ Telephone Interview
- ☐ Website/E-Form

1. DD Form 2807-1, Report of Medical History, OMB No. 0704-04132.
2. DD Form 2807-2, Medical Prescreen of Medical History, OMB No. 0704-04133.
3. DD Form 2008, Report of Medical Examination.
4. USMEPCOM Form 680-3A-E, Request for Examination.
5. USMEPCOM Form 601-23-E, Report of Additional Disclosures.
6. DD Form 1966/1-4, Record of Military Processing Armed Forces of the United States, OMB No. 0704-01737.
7. DD Form 4/1 & 2, Enlistment/Reenlistment document-Armed Forces of the United States.
8. DD Form 4/3, Enlistment/Reenlistment document-Armed Forces of the United States.
9. DD Form 93, Record of Emergency Data.
10. DD Form 1304-2AS, Enlistment Answer Sheets.
11. DD Form 1304-5AS, Student Answer Sheets.

12 USMEPCOM Form 611-1-20, Special Purpose Test Examination (NOTE: Data entered manually).
13 AIMS Form 1, AIM Answer Sheet.14. DD Form 398-2, National Agency Questionnaire, OMB No.0704-0298

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 A0601-270 USMEPCOM DoD

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. DAA-AU-2015-0010

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

(3) Retention Instructions.

DAA-AU-2015-0010-0001 Destroy immediately after applicant turns 43 years old.
DAA-AU-2015-0010-0002 Destroy 99 year(s) after applicant's disqualification date.

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.

a. Executive Order 13478—Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers
b. 10 U.S.C. 3013, Secretary of the Army
c. 10 U.S.C. 8013, Secretary of the Air Force
d. 10 U.S.C. 5013, Secretary of the Navy
e. DoD Directive 1145.02E, "United States Military Entrance Processing Command (USMEPCOM)," Ch 1 Effective May 22, 2018
f. DoD Directive 1304.12E, "DoD Military Personnel Accession Testing Programs," dated September 20, 2005
g. DoD Directive 1304.26, "Qualification Standards for Enlistment, Appointment and Induction," dated October 26, 2018 (Change 3)
h. DoD Instruction 4000.19, "Interservice and Intragovernmental Support," dated December 16, 2020
i. DoD Instruction 6130.3, "Medical Standards for Appointment, Enlistment, or Induction in the Military Services" dated April 30, 2021(Change 2)
k. USMEPCOM Regulation 680-3, Personnel Information Systems Entrance Processing and Reporting System Management, dated October 24, 2018

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.

0704-0413, DD Form 1966

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

Aptitude Test Results, Alien Registration Number, Recruit Identification Number
Primary Index Key: Applicant Identification Number
Secondary Index Key: SSN

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 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.

USMEPCOM Commander, Col Richard Brady, USMC, August 18, 2020.

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

SSNs are required for positive identification of military applicants since they are not yet members of the Armed Forces.

(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".

SSNs are used only when absolutely necessary within the system and through data exchanges with approved mission partners.

(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

SSNs are required and used in conducting background chcks and employment contract DD Form 4, Enlistment/Reenlistmenet Document Armed Forces of the United States. These are required in order to enter the all volunteer force.

b. What is the PII confidentiality impact level[2]? [ ] Low [ ] Moderate [X] 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
- [ ] Key Cards
- [ ] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [ ] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

This modified system is housed in Amazon Web Services GovCloud West. AWS is FedRAMP Impact Level 4 certified. Physical security controls, to include those associated with protection of Privacy data, are inherited.

(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
- [x] If Other, enter the information in the box below

All personnel (Military, Civilian, and Contractor) are required to have appropriate background checks conducted before accessing the systems. Privileged Users are required to attain and maintain certification in accordance with DoD 8140.01 and DoD 8570.01-M.

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

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

Regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). USMEPCOM accession partners are provided information through a secure Application Programming Interface through the Non-classified but Sensitive Internet Protocol Router Network (NIPRNET). Files transferred across the Internet/NIPRNET are encrypted using VPN or AES 256-bit encryption.

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