PRIVACY IMPACT ASSESSMENT (PIA)

For the

USMEPCOM Integrated Resource System (USMIRS)
United States Military Entrance Processing Command (USMEPCOM)

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 81 (DA00097)

☐ **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 007-21-01-20-01-1191-00-201-067

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 A0601-270 USMEPCOM DoD

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.

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	0704-0413, DD Form 2807-2
Enter Expiration Date	October 31, 2017

☐ **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.

a. E.O. 9397 (SSN) as amended
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)," dated January 8, 2005
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 September 20, 2011 (Change 2)
h. DoD Instruction 4000.19, "Interservice and Intragovernmental Support," dated August 9, 1995
i. DoD Instruction 6130.3, "Medical Standards for Appointment, Enlistment, or Induction in the Military Services" dated September 13, 2011 (Change 1)
j. Army Regulation 601-270/Air Force Regulation 33-7/Marine Corps Order P1100.75A, Military Entrance Processing Station (MEPS)
k. USMEPCOM Regulation 680-3, U.S. Military Processing Command Integrated Resources System (USMIRS)

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.

US MILITARY ENTRANCE PROCESSING COMMAND INTEGRATED RESOURCE SYSTEM (USMEPCOM MIRS): MIRS provides the automation and communications capability for USMEPCOM to meet its peacetime, mobilization, and wartime military manpower accession mission for the Armed Services. The mission of USMEPCOM is to ensure applicants entering into the Military Service meet the Service qualification standards. The automation USMEPCOM currently uses to collect applicant qualification information is the USMEPCOM Integrated Resources System (USMIRS).

USMEPCOM conducts its work through 65 MEPS across the United States and Puerto Rico. The main objectives of the 65 Military Entrance Processing Stations (MEPS) is to conduct aptitude tests, medical examinations, and administratively process, enlist, and ship applicants for the Armed Forces and Reserves; conduct aptitude tests, medical examinations and determine acceptability, administratively process, allocate, induct and ship Selective Service System registrants, when required; and provide aptitude and medical examination services for other Federal agencies, as requested MIRS interfaces with recruiting capabilities for the services, incorporating the concept of electronic data sharing using standard Department of Defense (DoD) data elements between USMEPCOM and all the Armed Services recruiting and accession commands.

In the event a military draft is required, MIRS directly supports mobilization through electronic links with the Selective Service system and its ability to provide processing and shipment to boot camp capability for those drafted into military service.

The type of PII collected is personal, financial, medical, employment, educational, and military.

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

Appropriate safeguards are in place for the collection, use, and sharing of information. Individuals who object to providing required information may be unable to enter the Armed Forces. Security measures are adequate and risk is minimal. Information is protected by user passwords, firewalls, antivirus software, CAC access, host-based intrusion prevention, network intrusion prevention, access control lists, and data-at-rest protection on workstations and laptops.

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. 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.**

Specify. Air Force Reserve Command (AFRC), Air Force Recruiting Information Support System (AFRISS), Marine Recruiting Information Support System (MCRISS), Navy Drub Screening Lab (NDSL), and Navy Recruiting Accession Management System (NRAMS)

☒ **Other Federal Agencies.**

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, Defense Health Agency (DHA)

☒ **State and Local Agencies.**

Specify. Army Reserve National Guard

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

Specify.

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

Specify.

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.

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

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

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.

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

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.

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.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☒ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☒ Citizenship	☒ Legal Status	☒ Gender
☒ Race/Ethnicity	☒ Birth Date	☒ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☐ Personal Email Address
☒ Mailing/Home Address	☒ Religious Preference	☐ Security Clearance
☒ Mother's Maiden Name	☒ Mother's Middle Name	☒ Spouse Information
☒ Marital Status	☒ Biometrics	☒ Child Information
☐ Financial Information	☒ Medical Information	☐ Disability Information
☒ Law Enforcement Information	☐ Employment Information	☒ Military Records
☒ Emergency Contact	☒ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	Aptitude Test Results, Alien Registration Number, Recruit Identification Number Primary Index Key: Recruit Identification Number Secondary Index Key: SSN

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Personal information is provided by individuals and Service recruiters. USMIRS information is collected using a paper-based collection via forms and electronic documents generated in Microsoft Office product suite formats, Jetform forms software, and Adobe LiveCycle forms software. Information is entered directly from Service recruiters and liaisons via electronic systems.

(3) How will the information be collected? Indicate all that apply.

☒	**Paper Form**	☒	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

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.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

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.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☒ **Yes** ☐ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

USMEPCOM Business Intelligence System is used for data aggregation, i.e. a process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. Summary data on applicants is collected from PII data on applicants.

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups

based on specific variables such as age, profession, or income.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☒ **Other**

Software Quality Assurance personnel

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒ **Security Guards**	☒ **Cipher Locks**
☒ **Identification Badges**	☐ **Combination Locks**
☒ **Key Cards**	☐ **Closed Circuit TV (CCTV)**
☒ **Safes**	☒ **Other**

All USMIRS servers are stored either in a data center or locked server/communications room.

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**	☒ **Biometrics**
☒ **Password**	☒ **Firewall**
☒ **Intrusion Detection System (IDS)**	☒ **Virtual Private Network (VPN)**
☒ **Encryption**	☒ **DoD Public Key Infrastructure Certificates**
☒ **External Certificate Authority (CA) Certificate**	☒ **Common Access Card (CAC)**

☒ **Other**

There is weekly monitoring and immediate disabling of accounts with easily guessed passwords, daily notifications of inactive accounts and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). USMEPCOM accession partners are provided information through regularly scheduled file transfers accomplished via sftp or email across the RSN or Non-classified but Sensitive Internet.

Protocol Router Network (NIPRNET). Files transferred across the Internet/NIPRNET are encrypted using VPN ore AES 256-bit encryption.

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

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.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	May 15, 2018
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection - Each MEPS retains a copy of reporting system source documents for each enlistee for 90 days after shipment. For all other applicants, each station retains, if applicable, a copy of the Report of Medical Examination (DD Form 2808) with supporting documentation,

Retention/Destruction - the Report of Medical History (DD Form 2807), and any other reporting source documents, for a period not to exceed 2 years unless the applicant failed to meet minimum medical enlistment standards which are kept for 7 years, after which they are destroyed.

Processing - Originals or copies of documents are filed permanently in the Official Personnel Files for acceptable applicants and transferred to the gaining Armed Forces Component.

Test score transmittals and qualification test answer records are maintained for one year and then destroyed. Test material inventory files are maintained until inventory is approved and destroyed when no longer needed for conducting business, but not kept for more than 6 years.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Two factor authentication, Least Access Privilege, secure/encrypted communication, auditing

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Does not apply.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	MORGAN.KENT.L.1139876942 Digitally signed by MORGAN.KENT.L.1139876942 Date: 2018.10.01 15:30:27 -05'00'
Name:	Kent L. Morgan
Title:	Chief Information Officer/Director J-6, Information Technology
Organization:	United States Military Entrance Processing Command
Work Telephone Number:	(847)-688-3680 x7701
DSN:	792-3680 x7701
Email Address:	kent.l.morgan.civ@mail.mil
Date of Review:	1 October 2018
Other Official Signature (to be used at Component discretion)	BANDY.LESLIE.ROY.1007370659 Digitally signed by BANDY.LESLIE.ROY.1007370659 Date: 2018.08.08 11:13:09 -05'00'
Name:	Leslie R Bandy
Title:	FOIA/Privacy Officer
Organization:	United States Military Entrance Processing Command
Work Telephone Number:	(847) 688-3680 x7182
DSN:	792-3680 x7182
Email Address:	leslie.r.bandy.civ@mail.mil
Date of Review:	

Other Official Signature (to be used at Component discretion)	GOSS.JODI.L.1291024307 Digitally signed by GOSS.JODI.L.1291024307 Date: 2018.10.05 10:14:17 -05'00'
Name:	Jodi L. Goss
Title:	Program Information System Security Manager, Chief, J-6/Cyber Security Office
Organization:	United States Military Entrance Processing Command
Work Telephone Number:	(847) 688-3680 x7722
DSN:	792-3680 x7722
Email Address:	jodi.l.goss.civ@mail.mil
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Privacy Officer Signature	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Component CIO Signature (Reviewing Official)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.