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:

Measurement Assessment and Research System (MARS)

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

02/19/21

HQDA DCS-G1, U.S. Army Research Institute for the Behavioral and Social Sciences

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

☐ 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

☐ 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 Measurement Assessment and Research System (MARS) application is a platform for Army Research Institute for hosting on-line data collection tests, measures, and surveys related to the military service. The data collection includes both service members and non-service members. DoD ID (EDIPI) will be used for identifying the survey respondent to their results, which means the information is not anonymous. However, due to the safeguards in place, only those authorized (based on credentials and registration to the MARS system) to the particular survey can access that ID. Other types of data to be collected from survey, test, etc. takers may include names, position, rank, duty location, employment information and demographic information. EDIPI will also be collected on those using the system for verification, identification, and authentication.

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)*

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Current and former officer, warrant officer, and enlisted military personnel, including Army Reservists and National Guard; civilian employees or contractors of Department of Defense.

CATEGORIES OF RECORDS IN THE SYSTEM:
Service member: Individual's name and EDIPI, Army personnel information and questionnaire-type data relating to service member's pre-service education, work experience and social environment and culture, learning ability, physical performance, combat readiness, discipline, motivation, attitude about Army life, and measures of individual and organizational adjustments; personnel test responses.

Non-service member: Individual's name and questionnaire type data relating to non-service member's education, work experience, motivation, measures of individual and organizational adjustments, knowledge of and attitude about the Army. When records show military service or marriage to a service member, the appropriate non-service records will be linked to the service record.

MARS SYSTEM ADMIN USERS:
EDIPI will also be collected on those using the system for verification, identification, and authentication; name, and DOD employee or contractor status.

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.

A survey taker can object to the collection of their information when the PAS is presented to them, and they will not move forward with the survey. Respondents may also opt not to answer particular survey questions, and to stop taking the survey at any time. All surveys executed in the MARS application are voluntary. Each survey will have a tailored version of the ARI SORN Privacy Act Statement, and if considered research, an informed consent, in addition to the PAS.

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.

A survey taker can consent to the uses of their PII as outlined in the specific survey's PAS and/or research informed consent document. Each survey will have a tailored version of the ARI SORN Privacy Act Statement, and if considered research, an informed consent, in addition to the PAS.

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 3013, Secretary of the Army;
10 U.S.C. 2358, Research and Development Projects; and
E.O. 9397 (SSN), as amended.

PURPOSE(S):
To research manpower, personnel, and training dimensions inherent in the recruitment, selection, classification, assignment, evaluation, and training of military personnel; to enhance readiness effectiveness of the Army by developing personnel management methods, training devices, and testing of weapons methods and systems aimed at improved group performance. (No decisions affecting an individual's rights or benefits are made using these research records).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:
In addition to the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The DoD Blanket Routine Uses set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

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.	Army agencies: Army Analytics Group, Assistant Secretary of the Army for Manpower and Reserve Affairs (ASA(M&RA)); Other Army agencies that would obtain access to information in this system, on request in support of an authorized investigation or audit, may include Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, and US Army Intelligence and Security Command.
☒ Other DoD Components	Specify.	Other DoD agencies on request, in support of an authorized investigation or audit, may include the individual's chain of command, Inspector General, law enforcement and criminal investigative agencies, and intelligence personnel.
☒ Other Federal Agencies	Specify.	As specified in the routine uses of the SORN.
☒ State and Local Agencies	Specify.	As specified in the routine uses of the SORN.

☒ 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. All contracts that require access to data in MARS will contain FAR and DFARS clauses requiring contractors to maintain required safeguards and will include the statement "The Contractor shall use appropriate safeguards to prevent use or disclosure of Personally Identifiable Information and Protected Health Information." In accordance with DoD regulations on Nondisclosure Agreement and Acceptable Use Policy, all contractors are required to agree to protect PII and comply with safeguards required under the related FAR/DFARS clauses..

☐ 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

☐ Face-to-Face 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

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier A0602 AHRC-ARI

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. Unscheduled - under RMI

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

(3) Retention Instructions.

Treat records as permanent. Do not destroy until schedule is approved.

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. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; 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 collection from non-service members will obtain OMB approval prior to initiation for each specific collection effort. Information collection from service members does not require OMB approval.

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)*

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

Psychological questions pertaining to people's attributes, opinions, behaviors, and actions in and/or towards the military service; Self-report of count and nature of Disciplinary information (e.g., Article 15's); Self-report information on the number and nature of assignments (e.g., deployments, command, joint/interagency, overseas); self-report information on the number and gender of dependent children; self-report information on financial status (e.g., ability to pay all bills, perceived need for working a second job, etc); Unit identifying information (e.g., UIC or alphanumeric unit identification information); contact information for peers, supervisors, subordinates, senior raters. Project specific constructed ID numbers may be used to facilitate matching data across multiple data collections or respondents in lieu of DOD ID in some instances.

* Although the SORN allows for collection of SSNs, ARI will *not* collect or store SSNs in MARS.

** Research studies and information collections within this system are reviewed under the Army and DOD Human Subjects Protection Program (32 CFR 219, DoDI 3216.02, ALARACT 031/2008) to minimize risk to research participants.

*** The system owner, organizational privacy officer and PISSM concur in judgment that the privacy impact level of this system is MODERATE based on the information provided here, and the governance/review process under the Army HRPP.

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?

☐ Yes ☐ No

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

n/a - ARI will *not* collect or store SSNs in MARS.

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

n/a - ARI will *not* collect or store SSNs in MARS.

(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".

n/a - ARI will *not* collect or store SSNs in MARS.

(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 □ No

n/a - ARI will *not* collect or store SSNs in MARS.

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

The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organiz

[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

□ If Other, enter the information in the box below

The information itself is collected in an electronic database with limited access (see below).
The MARS servers are located in the ADCF-E computer room of the AAG facility at 5253 Business Center Dr., Suite A, Fairfield, California. This is a controlled facility within a single-level office building. The AAG offices are secured by physical keypad entry control access, an active alarm system and 24 x 7 security monitored by the Department of Homeland Security (DHS), and local fire department response. This building houses the workspaces of the MARS application and database maintenance personnel.
The routers, switches, and servers in the ADCF-E enclave TLA Stack/DMZ are owned by AAG and maintained by the Army 7th Signal Command's Regional Cyber Center (RCC) for border control and by AAG for internal routing control. RCC provides monitoring services for the ADCF-E, including HBSS services.

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

☒ Backups Secured Off-site

☒ Encryption of Backups

☒ Methods to Ensure Only Authorized Personnel Access to PII

☒ Periodic Security Audits

☒ Regular Monitoring of Users' Security Practices

□ If Other, enter the information in the box below

We routinely verify user access to ensure they still require access in their current duty position. Information assurance and security awareness training is administered by the Information Management Office (IMO) at in-processing and on an annual basis. Backups of the MARS data and servers is maintained for 30 days in a secure off site location. All backups are encrypted using TDE.
Access to the computer room is restricted to operations and management who DoD 2875 complaint and having a minimum security clearance of Secret. Access to the computer room is controlled via CAC, all individuals must CAC into and out of the data center. Individuals are requiring access to the computer room who are not on the authorized access list must be signed in and out of the computer room by an individual authorized to escort service technicians, etc. Computer room access logs are reviewed monthly.

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

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

a. Encryption of Data at Rest – MARS data is stored in an Oracle and SQL database utilizing transparent data encryption (TDE). ADCF-E requires all data to be store encrypted regardless of the type of data. The MARS application inherits this control from ADCF-E.

b. Firewall – Access control Lists (ACL) are implemented across the enclave providing a layered defense. In addition to network ACLs, the project resources (servers and databases) utilize ACLs limit what resources can connect to them.

c. Role-based Access Controls - the MARS application employees role-based access control to limit users' permissions and access to need-to-know based on the role the user has be authorized to. The following roles are available in the MARS application: Administrator, Developer, and IRB Member, Unit Chief, and Survey participant.

d. Virtual-Private Network (VPN) – MARS Application is independent of the ADCF-E VPN. Remote access and/or administration of MARS and the system resources utilized by MARS is not allowed. Controls requiring the local administration of the system resources (networks, servers, database, etc.) is inherited from the ADCF-E. The ADCF-E VPN is utilized by the Army Analytics Group (AAG) System Administrators for the administration of the resources that the MARS system utilizes, for example network equipment, servers and databases. Connectivity to the ADCF-E VPN is limited to Army Analytics Group (AAG) personnel.

e. Common Access Card (CAC) – MARS application restricts access to users presenting a valid CAC. The Microsoft Internet Information Services (IIS) is configured by AAG to require that the CAC PKI certificate status is validated with the DoD certificate revocation list (CRL) via Online Certificate Status Protocol (OCSP) before the MARS application is rendered to the user web browser. The DoD CAC is utilized for non-privileged access to the MARS application. For privileged access to resources, (network devices, servers, databases, etc.) ADCF-E requires System Administrators to utilize DoD Privileged Tokens (ALT Tokens). Controls requiring the utilization of CAC and ALT-Token for two-factor authentication is inherited from ADCF-E.

f. Encryption of Data in Transit – MARS application use transport layer security (TLS) to encrypt the data in transit between the application server and the clients' web browser. Further, the connection between the application server and the database server is encrypted using TLS. ADCF-E requires all data in transit to be encrypted. The MARS application inherits this control from ADCF-E.
g. Intrusion Detection System – MARS application source code scanned annually and/or before the deployment of a new release of the application to production for potential vulnerabilities. Additionally, the MAR application and servers are scanned and inspected for potential exploits and vulnerabilities by AAG Information Assurance Specialist. All category 1 findings are required to be fixed before the AAG Application Configuration Control Board (ACCB) will approve the deployment of the application.

ADCF-E requires that all servers include DoD's Host Based Security System (HBSS) that provides intrusion detection and intrusion prevention. The MARS application inherits this control from ADCF-E.

h. DoD Public Key Infrastructure Certificates and External Certificate Authority Certificates – the MARS application utilizes both DoD and commercial certificates. DoD certificates are utilized to encrypt data in transit between servers with TLS. Commercial certificates are utilized by the MARS web application for encrypting the data in transit between the users' browser and the web server with TLS.
i. Least Privilege Access – the MARS application employees RBAC to ensure users accessing MARS are restricted to the functions and data within MARS based on their need-to-know. ADCF-E policy requires a separation of duties (SOD) for system administrators (privileged users). Quarterly the P-ISSM reviews the privileged access roster for conflicting duties. System admins supporting roles with conflicting duties requires approval of the P-ISSM.
j. The AADR application is tested, hosted, and maintained at the Army Analytics Group (AAG). All AAG personnel authorized to view AADR data possess a Secret clearance, at minimum. The AAG Test Environment is located on a DMZ subnetwork, physically separated from the AAG production network, and has layered protection provided by firewalls, switches, and whitelisting.

Access to the project database is restricted to local access only, no remote administration /access is permitted. Controls requiring all ACL

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

All data collected from the MARS application system are stored on secure network servers at Army Analytics Group (AAG). Firewall and intrusion detection systems are active and continuously monitored. Information assurance and security awareness training is administered by the Information Management Office (IMO) at in-processing and on an annual basis. Files with sensitive data have restricted access and the Common Access Card (CAC) login is enforced. Hypertext Transfer Protocol Secure (HTTPS) is used with the Secure Sockets Layer (SSL)