PRIVACY IMPACT ASSESSMENT (PIA)

For the

Marine Corps Training Information Management System (MCTIMS)
United States Marine Corps

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	8712
☐	**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 007-17-01-03-02-2414-00

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 NM01500-2

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

Enter Expiration Date

☒ **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.

(1) 10 U.S.C. 5041, Headquarters, Marine Corps
(2) 10 U.S.C. 5013, Secretary of the Navy
(3) EO 9397
(4) OPNAVINSTR 1510.10B - CETARS, Catalog of Navy Training Courses and Student Reporting Requirements
(5) MCO 1560.7J Inter-Service Training

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.

MCTIMS is a web-based application which maintains the integration of training functions and data, training standards (Training and Readiness manuals), Military Occupational Specialty (MOS) manual and Roadmaps, individual Marine and other Service personnel Electronic Training Jacket, and automated tools in a single, consolidated database. MCTIMS is available to authorized Marine units/activities or other Services world-wide, 24 X 7 using standard web tools. It fits within the Office of the Secretary of Defense (OSD) and Marine Corps objectives of providing a web-based Net-Centric, enterprise shared data environment, providing a principal Marine Corps Training Authoritative Data Source, allowing for unit Training Readiness Assessments, and supports unit Combat Readiness Assessments (CRA). It provides for Unit Training Management (UTM) support and future CRA.

The type of personal information collected in MCTIMS includes: Name, Rank, Social Security Number (SSN), MOS, Gender, Race, Dependent Information, Home Address, Unit Name and Address, Date of Rank, Future Duty Station Name and Address, Home of Record address or other additional address if taking leave en route to a new duty station and Training Completions and Scores.

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

As with many information technology systems, MCTIMS has potential privacy risks in the areas of identity theft, unsolicited marketing, loss of customer faith in protecting their information, and compromise of sensitive information. However, potential privacy risks are mitigated through access restrictions, user roles and permissions, and annual Privacy and PII training. MCTIMS is used exclusively by authorized military, DoD personnel, and contractors supporting DoD. Personally Identifiable Information (PII) is shared or released only after the individual has provided written consent using the standard Privacy Act Statement Release Form. Only those users with the Administrator role are able to provide access to the MCTIMS application. Access to MCTIMS is provided on a need to know basis and via a valid Public Key Infrastructure (PKI) enable authentication. All MCTIMS users (to include contractors) receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in MCTIMS. In addition, contractors receive an annual security briefing conducted by their companies Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

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.

PII will be shared with the following systems and their users/owners.

System: MarineNet
System Owner: USMC Training and Education Command (TECOM)

System: Marine Corps Recruiting Information Support System (MCRISS)
System Owner: Marine Corps Recruiting Command (MCRC)

System: Marine Corps Total Force System (MCTFS)
System Owners - Jointly: USMC Manpower & Reserve Affairs (M&RA)
& Defense Finance & Accounting Services (DFAS)

System: Operational Data Store Enterprise (ODSE)
System Owner: USMC M&RA

System: Total Force Data Warehouse (TFDW)
System Owner: USMC M&RA

System: Total Force Retention System (TFRS)
System Owner: USMC M&RA

☒ **Other DoD Components.**

Specify.

System: Army Training Requirements and Resources System (ATRRS)
System Owner: Army Training & Doctrine Command (TRADOC)

System: Corporate Enterprise Training Activity Resource Systems (CETARS)
System Owner: Naval Education & Training Command (NETC)

System: Defense Manpower Data Center (DMDC)
System Owner: DMDC

System: Sailor/Marine American Council on Education Registry Transcript (SMART)
System Owner: Navy College Center

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

Contractors sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information. Specific language in the contract is described as:

Security measures shall be taken to satisfy the security requirements in accordance with the Marine Corps System Security Plan. MCTIMS data/information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management.

MCTIMS will share PII with contractors who have a valid need to know and a favorably adjudicated background investigation. Contractors may be exposed to PII while testing and maintaining MCTIMS. A Secret clearance will be required for personnel requiring access to Information Technology Data Center, Quantico (ITDC-Q).

☐ **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.

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

Individuals do not have an opportunity to object to the collection of their PII in MCTIMS. PII is required for training and education activities. While PII must be collected, individuals are able to correct erroneous information resident within MCTIMS. PII for Marines and select Sailors is pulled from the ODSE system. PII for other Sailors (not resident in ODSE), government civilians, other Service personnel and foreign nationals are manually entered by school house administrators when they are registering for a school seat. Individuals whose information is pulled directly from ODSE and notice errors in MCTIMS, may initiate an update to the information by accessing the Total Force Administration System (TFAS) Marine Online (MOL) system. TFAS MOL allows Marines to update select biographical information.

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.

PII resident in MCTIMS is used to provide training management services for the individual, unit and formal schools world-wide. If a Marine or other Service personnel were given the opportunity to exclude their PII from MCTIMS, it would prevent them from being considered for selection to our formal schools within the Marine Corps as well as other Service schools. The individual would also be excluded from unit training and rifle/pistol qualifications. These exemptions would render our Marines ineligible for any promotions, retention and assignments, necessitating their discharge from the Marine Corps.

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 Service personnel and applicants for service sign their NAVMC 11000 Privacy Act statements which are maintained in their Service Record Books (SRB) or Officer Qualification Record (OQR) and cover the collection of PII in all DoD Automated Information Systems (AIS) to manage their military careers and the Services force structures. PII collected or pulled into MCTIMS is not disseminated to any individual, agency or system outside those already previously listed in this PIA, which has an interface with MCTIMS and functions as a part of the training evolution for career enhancement of the individual. The MCTIMS Program Manager is working with the HQMC Privacy Act Officer to create a MCTIMS Privacy Act Statement (PAS) for all MCTIMS users to acknowledge, each and every time a user logs into MCTIMS. This PIA will be amended once the PAS is published. All MCTIMS users (to include contractors) receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in MCTIMS. In addition, contractors receive an annual security briefing conducted by their companies Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

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.