PRIVACY IMPACT ASSESSMENT (PIA)

For the

Marine Corps Aviation Learning Management System - Enterprise (MCALMS-E)
Department of the Navy - United States Marine Corps (USMC)

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: 13968
- ☐ **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

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.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps function, composition
OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS)
Catalog of Navy Training Courses and Student Reporting Requirements
MCO 1580.7D Schools Inter-service Training
E.O. 9397 (SSN), as amended.

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 Marine Corps Aviation Learning Management System Enterprise (MCALMS-E) is a Web-based system designed to present learning and knowledge sharing opportunities to its target audience, primarily Marine Corps Aviation users, students, and Instructors, both in the field and in the schoolhouse. It has been specifically designed for a US DoD user environment providing learning and management tools for both self-paced and instructor led training content. MCALMS-E supports the ADL initiative through the delivery of SCORM compliant courseware as well as the delivery of other presentation media such as PowerPoint presentations, Seminars, Webinars and reference/resource sharing. MCALMS-E provides a complete and thorough version control system for both curricula and course content thereby supporting a continual update model. Other US Marine Corps required customizations include a proctored assessment control module for real-time assessment proctoring, specialized instructor interfaces for group presentations and student attendance, automated assessment online feedback and review, automated curriculum and course level critiques and surveys, dynamic user references as well as training administration features. MCALMS-E provides a fully managed administrative role based permission model as well as group and content level access control. MCALMS-E meets all DoD mandated security requirements including Public Key Infrastructure (PKI) and Command Access Card (CAC) authentication methods. MCALMS-E has the capability to interface with other Marine Corps systems such as Training Management Systems (TMS's) and Resource Management Systems (RMS's) in order to provide student training completion data and reoccurring certification completion data for input into a student's master training file. It also provides training metrics and custom reports using data that is current, accurate, and consistent.

Personal information collected in includes: Name, Social Security Number (SSN), Truncated SSN, Other ID Number, Home Telephone Number, Personal E-mail Address, Mailing/Home Address, Military Records (Service Branch, Pay Grade, Rank, MOS/AFSC/NEC, Organizational Unit Name, Training Completions and Scores).

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.). All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that MCALMS-E information could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since MCALMS-E operates on the NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset. All systems are vulnerable to "insider threats". MCALMS-E managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to this system. These individuals have gone through extensive background and employment investigations.

MCALMS-E has the potential for privacy risks in the areas of identity theft, and compromise of sensitive information as does any IS system. In order to minimize these risks, one method of mitigation for PII data within MCALMS-E is that all Personally Identifiable Information (PII) data is encrypted using a 256 bit encryption during transmission and all users SSN's and Electronic Data Interchange Personal Identifier's (EDIPI) are encrypted again using a 128 bit 3Des encryption while at rest in the database. Appropriate safeguards are in place for the collection, use, and sharing of information. Any potential privacy risks are mitigated through access restrictions, user roles and permissions, and annual Privacy and PII training. MCALMS-E is used exclusively by authorized military, DoD personnel, and contractors supporting DoD. Only those users with the System Administrator or System Registrar roles are able to provide access to the MCALMS-E system. Access to MCALMS-E is provided on a need to know basis only. Access to MCALMS-E is controlled through the use of a valid Public Key Infrastructure (PKI) certificate or Command Access Card (CAC). All MCALMS-E users, including contractors, receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in MCALMS-E. In addition, contractors receive an annual security briefing conducted by their respective 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 only be shared to authorized users with a need to know in order to perform official government/DoD duties. Information from the MCALMS-E system is shared among the U.S. Marine Corps and U.S. Navy communities consisting of Naval Education and Training Command (NETC), Center for Naval Aviation and Technical Training (CNATT), Marine Corps Training and Education Command (TECOM), Chief of Naval Air Training (CNATRA), Marine Corps Commandant, Chief of Naval Operations, U.S. Naval Criminal Investigative Command, U.S. Naval/Marine Corps Mishap Board, and U.S. Naval Intelligence and Security Command.

☒ **Other DoD Components.**

Specify. Other internal DoD agencies that may need to obtain PII from the MCALMS-E system, on request and in support of an authorized investigation could include Under Secretary of Defense for Personnel & Readiness, and Defense Manpower Data Center.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **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.

(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 MCALMS-E. PII is required for training and education activities. While PII must be collected, individuals are able to correct erroneous information resident within MCALMS-E. PII for active duty service personnel, government civilians, other Service personnel and possibly foreign nationals are manually entered by school house system administrators or registrar's when they are registering for a MCALMS-E seat.

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 MCALMS-E 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 MCALMS-E it would prevent them from being considered for selection to formal schools within the Marine Corps as well as other Service schools. The individual would also be excluded from unit training. 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 official MCALMS-E users receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard PII. In addition, contractors who have access to the system also receive an annual security briefing conducted by their company's Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding and storing of PII data.

All official MCALMS-E users are required to read and acknowledge a U.S. Government (USG) Information System (IS) prior to entering into the MCALMS-E system, which notifies the official user that they are entering into an official USG Information System and is provided for USG authorized use only, and is routinely monitored.

All official MCALMS-E users are required to read and acknowledge a Privacy Act Warning (PAW)

statement prior to entering into the MCALMS-E system, which notifies the official user that they are entering into a system that is governed by rule-making established by the Privacy Act of 1974 [5 U.S. C. 552a] and that mandated safeguarding, handling and disposal procedures must be observed. The PAW further apprises the official user that they are not allowed to share or disseminate PII from MCALMS-E unless authorized by law and that civil and /or criminal penalties will apply.

All official MCALMS-E users are required to read and acknowledge a Privacy Advisory Statement (PAS) displayed to the official user prior to providing or updating their PII information records maintained in the MCALMS-E system.

All official MCALMS-E users are provided access to a Privacy & Security Policy Information page which upon selection, is displayed to the official user. The Privacy & Security Policy Information page provides a description on the use of Social Security Number (SSN) within MCALMS-E and provides information on system security practices and the use of all information collected in the MCALMS-E system.

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.