PRIVACY IMPACT ASSESSMENT (PIA)

For the

Marine Corps Equipment Readiness Information Tool (MERIT)
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	1628
☐	**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 007-17-01-64-02-1263-00

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 NM05000-2

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.

- 10 U.S.C. 5013 Secretary of the Navy
- 10 U.S.C. 5041, Headquarters, Marine Corps
- 10 U.S. Code (USC), Part 1 Chapter 506 Section 5042, in that, the Commandant of the Marine Corps will prepare for such employment of the Marine Corps, and for such recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering, and maintaining of the Marine Corps.
- E.O. 9397 (SSN).

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 goal of the United States Marine Corps (USMC) Marine Corps Equipment Readiness Information Tool (MERIT) sustainment effort is to streamline and improve the logistics support for fielded systems within the USMC by providing visibility of legacy systems data that can be used to:
- Identify readiness and sustainment issues
- Optimize support structure and costs
- Revise support structures when changes or deficiencies are identified
- Support the update of logistics products
- Accelerate logistics analysis
- Improve baseline logistics support systems for major new starts
- Create graphical logistics analysis views of USMC assets/organizations
- Generate historical readiness charts.

This application provides custom decision support and analysis tools that present a unified view of the USMC legacy systems' data used to forecast logistics support needs and to react to field-reported problems or deficiencies. Logistics analysts can retrieve information and generate analyses via a Web-based user interface and analysis engine that will access the Master Data Repository (MDR).

The intended users are any Marines, civilian Marines, or government contractors at any level of command who need access to supply and/or maintenance information for Marine Corps ground equipment. These users include, but are not limited to: supply personnel, maintenance personnel, logistics personnel, commanding officers, program managers, and item managers.

Personal information collected for user accounts: first and last name, address, job title, organization, unit, supervisor and sponsor name, phone number, e-mail address, and partial SSN.

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

SSN Removal Plan
Per Defense-Type Memorandum: (DTM) 07-015-USD (P&R) - "DoD Social Security Number (SSN) Reduction Plan" the removal of the last four of the SSN is required. A three phase approach is planned to minimize deployment schedule impact. There are three Life Cycle Modeling Integrator (LCMI) applications that store and manage user profile information including SSN; Asset Enterprise Management Information Tool (AEMIT), MERIT and the Master Scheduling Support Tool (MSST). The plan will define the process for removing SSN from all three of the LCMI applications. Since all the LCMI applications use a common user repository to store the user profile information, this plan has a three phase approach that consists of removing the SSN from the front end applications, removing the SSNs from the shared common user components, and then finally removing the back end database fields.

1. Remove the SSN data fields and labels from the AEMIT, MERIT and MSST applications. Remove the last four digits of the SSN.
2. Once all the applications (AEMIT, MERIT and MSST) have deployed with the removal of the last four digits of the SSN as described in Step 1, the SSN/PIN fields will "zero out" in the database and strip the SSN/PIN fields from the applications.
3. Remove the filed SSN/PIN field from the Database Administrator (DBA) tables.

Phase 1: Code Changes
This first phase removes the SSN from the following:
- User Application Process
- User Update Performance/Update Profile
- Administration Update User Profile
- Reset Password.

The update will only remove the "check" to determine if the SSN that was entered in the Forgot Password page matches what is in the database for that username.

Once this change is complete, this phase will be cloned on the AEMIT, MERIT, and MSST applications that perform the user authentication to have them implement the removal of the SSN from their pages and applications. All references to the PIN column in this package were either removed or changed to NULL. At the completion of this phase the PIN/SSN will not be displayed by the applications any longer, but the SSN/PIN data will remain in the database until all applications have completed Phase I.

Phase II: Database Work Only
This phase is database work only. All of the code was changed in Phase I. Phase II will remove the PIN columns from the database tables. Once this is complete the SSN values will be null in the database.

Phase III: Remove PIN Field and Simultaneous Deployment
This phase is just to remove the columns from the database and clean up the stored procedures to remove the SSN/PIN field nulled out in Phase II. This phase will mostly be database work and updates to some common components that all the applications use. As those components are updated the applications will need to be redeployed to incorporate the common component changes.

Description of privacy risks associated with Personally Identifiable Information (PII) and how these risks are addressed to safeguard privacy:
Access to MERIT is controlled through a tiered hierarchy of security measures. All user access must be through a Hypertext Transfer Protocol (HTTP) over Secure Socket Layer (SSL) connection. All data transmission, in and out of the Web site, is encrypted with the USMC standard 128-bit encryption. IAW DODI 8500.2 (DCMC-1)i.

DoD Firewall: MERIT is hosted on a secure USMC .mil domain and only authorized users with an approved account and valid Public Key Infrastructure (PKI) certificate can obtain access. IAW DODI 8500.2 (ECND-1)i, (ECND-2)i, (DCDS-1)i, (EBBD-1)i.

PKI Certification: Security is designed so that persons cannot obtain access to the MERIT application unless they have a valid Department of Defense (DoD) Common Access Card (CAC) with a personal security certificate installed. PKI certificates are verified for revocation status to insure users with revoked PKI certificates are denied access. Web browser access requests for the MERIT Web site will not reach the server unless valid certificates are installed and a CAC card is inserted prior to attempting to reach the Web server. Persons accessing the Web server without PKI validation are denied access to the MERIT server and routed to another computer for an error message. IAW DODI 8500.2 (DCMC-1)i, (DCNR-1)i, (IAKM-2)i, (IATS-2)i, (IAKM-1)i, (IATS-1)i.

User Accounts: Persons meeting the above criteria and able to access the MERIT Website may apply for a user account to enter the application. User access is regulated through PKI authentication. A user must access the Life Cycle Modeling Integrator (LCMI) Portal (LCMIP) home page and submit an application to the C4 Customer Service Center (located at MCLB Albany). Users must possess a valid DoD email account and provide detailed information to obtain account approval. IAW DODI 8500.2 (IAIA-2)c, (IAIA-1)c, (DCMC-1)i.

The MDR database servers are located behind the DoD, Navy Marine Corps Intranet (NMCI) and Marine Corps Logistics Base (MCLB) Albany firewalls. Access is controlled and available to the MERIT Web server. Oracle Advanced Security Option (ASO) encryption, a DoD approved encryption standard, is applied at the database and data transfer level. All data leaving the database for use by users connecting to the MERIT application is encrypted. All data requests coming to the database server from the Web server are also encrypted.
IAW DODI 8500.2 (ECSD-1)a.

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. System: MERIT
System Owner: Marine Corps Logistics Command (MARCORLOGCOM)

Module: Total Life Cycle Management-Common Operating Picture (TLCM-COP)
Module Owner: MARCORLOGCOM

Module: Total Support Cost (TSC)
Module Owner: MARCORLOGCOM

Module: Decision Support Tool Kit (DSTK)
Module Owner: MARCORLOGCOM

Module: Supply Chain Operation Performance Enabler (SCOPE)
Module Owner: MARCORLOGCOM

☐ **Other DoD Components.**

Specify.

☐ **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.

LCMI application access requirement.
Privacy Act Statement on the Access Application form:
"Disclosure of this information is mandatory; failure to provide the requested information will prevent further processing of the request."

This data is requested to approve and authenticate users to safeguard the system's administratively sensitive information. Failure to provide data will result in the inability to gain access to the system.

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.

This information is required to authorize user system access and to authenticate the individuals to safeguard the administratively sensitive information.

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.

Privacy Act Statement on the Access Application form: "Disclosure of this information is mandatory; failure to provide the requested information will prevent further processing of the request."

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.