PRIVACY IMPACT ASSESSMENT (PIA)

For the

Web-Based Manpower Assignment Support System (WEBMASS)
Department of the Navy - 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: DITPR ID: 4537 DITPR DON ID: 5731
- ☐ **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 UII: 007-000005763

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 M01040-3

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 M01040-3 authorities:

10 U.S.C. 5013, Secretary of the Navy;
10 U.S.C. 5041, Headquarters, Marine Corps;
10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas;
32 CFR 64.4, Management and Mobilization;
DoDI 1215.13, Reserve Component (RC) Member Participation Policy;
DoDI 3001.02, Personnel Accountability in Conjunction with Natural and Manmade Disasters;
CJCSM 3150.13B, Joint Reporting Structure Personnel Manual;
DoDI 6490.03, Deployment Health;
MCMEDS;
SECNAVINST 1770.3D, Management and Disposition of Incapacitation Benefits for Members of the Navy and Marine Corps Reserve Components (Renamed Line of Duty (LOD));
MCO 7220.50, Marine Corps Policy for paying Reserve Marines; and
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.

WebMASS is an integrated personnel management system that provides Marine monitors with the tools and information they need to make informed assignment and career management decisions; in addition to issuing and managing the orders that execute those assignments around the globe. There are approximately 250 Manpower Monitors and support personnel who access WebMASS to generate approximately 50,000 Permanent Change of Station Orders (PCSO) annually. WebMASS enables Monitors to effectively manage thousands of jobs and billets through sourcing the right Marine to the right billet at the right time.

Personal information collected: Name, SSN (full and truncated), Other ID: DoD ID number, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, home telephone number, mailing/home address, religious preference, security clearance, Spouse and Dependent Informtion: Exceptional Family Member Program (EFMP) data. Spouse SSN to facilitate Marine Corps Policy adherence for dual military household assignment, marital status, military records (Rank, Occupational Specialty (MOS), Unit Information, Date of Rank, Future Duty Station), Education Information(major of study, and level of degree completion).

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

To Reduce privacy risks, the USMC's personnel systems, namely MCTFS and ODSE, have implemented the DoD ID number, a new unique identifier for personnel, which has replaced the SSN for identification of personnel. WebMASS will require the need to display truncated SSNs and use of the full SSN for individuals who do not have a DoD ID number. WebMASS release 3.0.1.0 replaced SSNs with DoD ID numbers. However, SSNs do remain stored in a WebMASS database to send to the Marine Corps Total Force System (MCTFS). MCTFS needs these SSNs as pay and entitlements are reported to the Social Security Administration and Internal Revenue Service; which only recognize the SSN as a personal identifier.

As with many information technology systems, WebMASS 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. WebMASS is used exclusively by HQMC Manpower Monitors, their administrative support personnel, and contractors supporting the Monitors mission. SSNs are available only to the Administrators on the application side.

Personally Identifiable Information (PII) is not shared or released to any individual, business, organization, entity, or agency outside those exclusively listed in Section 2, paragraph h below. Only those users with the Administrator role are able to provide access to WebMASS. Access to WebMASS is provided on a need to know basis and via a valid Public Key Infrastructure (PKI) enable authentication. All WebMASS users (to include contractors) receive mandatory Marine Corps sponsored Privacy Act and PII protection and breach training annually to help safeguard the PII resident in WebMASS. 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: Total Force Data Warehouse (TFDW)
System Owner: USMC, M&RA

System: Marine Corps Total Force System (MCTFS) - VIA UD/MIPS.
System Owner: USMC & M&RA

System: Unit Diary / Manpower Integrated Personnel System (UD / MIPS)
System Owner: USMC & M&RA

System: Marine Corps Permanent Duty Travel (MCPDT)
System Owner: USMC & M&RA

☐ **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.

WebMASS contractors sign a Non-Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information as per their MARCORSYSCOM contract M67854-14-D-4802, Delivery Orders 0036, 0035 and 0039.

Specific language in the contract is described as:

PDSS Roles and Responsibilities will be assigned. All individuals working the contract must have PDSS Security Clearances and Certifications. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD.

The contractor must have evidence of Secret Individual Clearance for any privileged users and/or individual with root access for the WebMASS NIPRNET enclave. The WebMASS contractor shall have, and provide evidence of, necessary Cybersecurity certifications as appropriate for privileged users supporting the system. Provide awareness and prevention through assessment and implementation of best practices (code reviews, system scans, vulnerability alerts, vendor notifications, Security Technical Implementation Guides (STIGs)). Implement cybersecurity best practices to increase the security of the system and eliminate vulnerability threats to include code reviews, system scans, vulnerability alerts, vendor notifications and STIGs.

The contract contains the required Privacy Act FAR clauses.

☐ **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.

PII is not collected directly from the individual.

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 is not collected directly from the individual.

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. WebMASS does not collect PII directly from the individual.

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.