PRIVACY IMPACT ASSESSMENT (PIA)

For the

MANPOWER INFORMATION PORTAL VERSION 1.0.x.x
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	DADMS ID: 46545
☐	**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 M01040-2

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. 03/19/2010 Pending Approval

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.

Executive Order 9397 of 23 November 1943, allows a federal department to utilize social security numbers as account numbers for individual persons;

Title 10 USC, Part I, 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;

Title 10 USC 5013, in that the Secretary of the Navy is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Navy, including the following functions: recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering (including the morale and welfare of personnel and maintaining.;

10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas

10 U.S.C. 5013, Secretary of the Navy

10 U.S.C. 5041, Headquarters, Marine Corps

32 CFR 64.4, Management and Mobilization.

DoD Dir 1215.13, Reserve Component Member Participation Policy

DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural and Manmade Disasters

CJCSM 3150.13B Joint Reporting Structure – Personnel Manual

DOD Instruction 6490.03, "Deployment Health," August 11, 2006

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

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 Manpower Information Portal provides the Marine Corps with the ability to support and manage all aspects of the Human Resource Development Process (HRDP) of all Active Duty and Reserve Marines. The system also includes the capability to report certain entries to enhance personnel management for reserve and retired Marines, Government employees working for the Marine Corps, other DoD military personnel, as well as Foreign Military Service personnel who are attached to Marine Corps commands. In addition, it has the capability to provide simulation, analysis, and forecasting tools to capture and process manpower information, making data visible to the appropriate Marine Corps decision makers, as well as providing statutory and regulatory management reports to higher headquarters.

The MIP system collects PII in the form of: Name, SSN, biometric information, address, phone, financial information, medical information, employment information, education information, DOB, dependent information and all data elements found in ODSE. See section three of this PIA for a complete list.

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

Risk:

Records are retrieved by name and/or Social Security Number.

Safeguards:

Logging into the system or the network requires the use of the DoD Common Access Card (CAC). Public Key Infrastructure (PKI) network login may be required to allow for documents to be digitally signed and encrypted and/or the receiving of encrypted mail. All official users use the CAC and PKI to login to their computer, digitally sign and encrypt e-mail and other documents used to establish secure internet sessions.

Access to server rooms, are strictly controlled by the hosting facility personnel in accordance with established Navy/Marine Corps security and access procedures. At a minimum, cipher locks, access rosters, sign-in sign-out procedures, escort and supervision of all maintenance personnel and physical security checks are provided on a routine basis. Physical security of buildings after normal working hours, are provided by independent security guards or military police. Periodic and unannounced audits to ensure compliance of security procedures are conducted at least quarterly.

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. Navy

☐ **Other DoD Components.**

Specify. Army, Air Force and other entities within the DoD

☒ **Other Federal Agencies.**

Specify. National Archives (Awards)

☐ **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.

MIP does not collect PII directly from the individual. The "Gold Source" of data is the Operational Date Store Enterprise (ODSE), which in accordance with the USMC rules for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5E; 32 CFR part 701; or may be obtained from the system manager

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.

MIP does not collect PII directly from the individual. As data is shared from the centralized manpower databases (ODSE and MCTFS), individuals are not provided the opportunity to object to the data collection. The Marines do not have the opportunity to object to PII within MIP, however they do have the opportunity to object to information in MCTFS at anytime. An annual audit of MCTFS is conducted to give members the opportunity to review their information and update it as necessary. A Marine can also view their individual record through the Total Force Administration System (TFAS) Marine OnLine (MOL) application which is a self-service personnel portal.

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.

MIP does not collect PII directly from the individual.

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. All individuals receive a Privacy Act Statement each and every time their personal information is collected.

All Marines receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

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:

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. MIP information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management.

Only contractors who have a valid need to know and a favorably adjudicated background investigation are permitted to have access to MIP. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting

the DoD.

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.