PRIVACY IMPACT ASSESSMENT (PIA)

For the

Marine Corps Force Augmentation Processing System (MCFAPS) Currently: Manpower Mobilization Assignment System (MMAS)
Department of 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

DITPR ID: 5037   DITPR-DON: 5747

☐ **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: 007-000005778

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 <u>retrieved</u> 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, U. S. Marine Corps
10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas
32 CFR 64.4 Management and Mobilization 5 U.S.C. Section 301, Departmental Regulations
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
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
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 purpose of the system is to provide support to Deputy Commandant, Manpower and Reserve Affairs (DC, M&RA), Manpower Management Integration Branch (MMIB); Force Augmentation.

MCFAPS provides capabilities in the management of the Individual Augmentation (IA) process as part of the Marine Corps total force mobilization, activation, integration, and deactivation plan. The IA process entails the assignment of active duty (Regular and Active Reserve (AR) and/or Reserve (IMA, IRR, SMCR or Retiree)) members to IA requirements.

The type of personal information about a Marine collected in MCFAPS includes: Name, Other names used, Full and truncated SSN, DoD ID number, Citizenship, Legal Status, Gender, Race/Ethnicity, Birth date, Place of Birth, Home Telephone Number, Mailing/Home Address, Marital Status, Financial information, Medical Information, Disability Information, Employment Information, Military Records, Emergency Contact Information, and Education Information.

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

The data contained in MCFAPS is exposed to privacy threats such as: identity theft, disgruntled employee, acts of nature (fire, flood, etc.), sabotage, computer hackers, and information warfare. To provide a layer of protection, access is provided on a need to know basis via a valid Public Key Infrastructure (PKI) solution.

Mitigation(s):
1) All MCFAPS users receive security training on a continuous basis to keep users alert to security requirements.
2) Access controls: Only users with Government approved accounts and a need-to-know are able to view data published by MCFAPS through a Public Key Infrastructure (PKI) Common Access Card (CAC) enabled authentication process. All MCFAPS users to include contractors receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually. This training for safe handling procedures cover receiving, viewing, printing, forwarding, storage and shredding of PII.
3) Confidentiality & Integrity: Only those users with the System Administrator role are able to provide access to MCFAPS. Access to MCFAPS is provided on a need to know basis and via a valid Public Key Infrastructure (PKI) enable authentication.
 Physical Security: MCFAPS is hosted in the Marine Corps Enterprise Information Technology Services (MCEITS) secure hosting facility located in Kansas City, MO.

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: Operational Data Store Enterprise (ODSE)
System Owner: USMC, Manpower & Reserve Affairs (M&RA)

System: Marine Corps Orders Resource System (MCORS)
System Owner: USMC, Manpower & Reserve Affairs (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.
[SAIC is the MCFAPS contractor. 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. MCFAPS data/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 MCFAPS. During the
course of routine system maintenance contractors may be exposed to PII. Users are
DoD employees or authorized contractors supporting the DoD.

The two FAR privacy clauses will be added when the contract is renewed.]

☐ **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.

PII is not collected 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.