PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAF Human Resource Management System (HRMS)
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: 4691 DITPR DON ID: 11346
- ☐ **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: 007-000006743

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 N12293-1/NM07010-1/NM07421-1

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:

N12293-1

5 U.S.C. 301, Department Regulations
5 U.S.C. Chapters 11, Office of Personnel Management
13, Special Authority
29, Commissions, Oaths and Records
31, Authority for Employment
33, Examination Selection, and Placement
41, Training; 43, Performance Appraisal
51, Classification
53, Pay Rates and Systems
55, Pay Administration
61, Hours of Work
63, Leave
72, Antidiscrimination, Right to Petition Congress
75, Adverse Actions
83, Retirement
99, Department of Defense National Security Personnel System

5 U.S.C. 7201, Antidiscrimination Policy
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness
E.O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended
29 CFR 1614.601, EEO Group Statistics
SECNAV Instruction 12250.6, Civilian Human Resources Management in the Department of the Navy
E.O. 9397 (SSN), as amended

NM07010-1

10 U.S.C. 5013, Secretary of the Navy
E.O. 9397 (SSN), as amended

NM07421-1

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
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.

To provide Human Resource information and system support for the USMC NAF civilian workforce worldwide to access and update their personal information, submit documents, and obtain personnel related information. To compute employees' pay entitlements and deductions and issue payroll checks for amounts due; to withhold amounts due for Federal, state, and city taxes, to remit withholding's to the taxing authorities, and to report earnings and tax collections; and upon request of employees, to deduct specified amounts from earnings for charity, union dues, and for allotments to financial organizations. It maintains time and attendance data and labor distribution data.

Personal information collected includes: Name, Social Security Number(SSN), citizenship, gender, race/ethnicity, birth date, place of birth, home telephone number, mailing/home address, security clearance, spouse information, marital status, biometrics, child information, financial information, medical information disability information, employment information, military records, emergency contact, education information.

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

Classification of Data processed and stored in HRMS is unclassified. The Health Insurance Portability and Accountability Act of 1996, HIPAA, defines the sensitivity of HR data. MCCS implements measures to safe guard data in compliance with HIPAA. Loss of any amount of data is unacceptable. HRMS data is essential for each individual employee and any large amount of data loss can have a severe impact to operations. The risk to HRMS is identical to the threat facing all network accessible applications whether government or commercial, classified or unclassified. Vulnerabilities exist in software applications, hardware infrastructure, operating system software, network & communications, business policy & procedures and in the nature of humans and organizations. Several threat agents can also act without being directed to specific targets and can potentially present threats to HRMS regardless of whether it is specifically targeted or not.

The risk is mitigated first and foremost with controlled access to the HRMS. These control measures begin at the physical entry points to the Marine base installations where employees are required to show appropriate personal identification. Once they are on the base installation entry to the building that is host to the HR business activity or

the IT support activity requires appropriate credentials and access permission with their common access card (CAC). Given building access they can logon to their government issued computer workstation only if permission has been authorized. To interface with any application specific permissions must be granted and furthermore various levels of permission are granted to each user depending on role & responsibility to control data access and application functions.

Risk is further mitigated with training of every HR staff employee on correct procedures and policy for handling PII for collection, system entry, record creation, and information management. The role and responsibility of each HR staff employee is granted to only those who satisfy the requisite skills and management practices. The risk to PII compromise or inappropriate dissemination is further mitigated by documented control measures and procedures IAW USMC standard procedures for handling and securing confidential and sensitive information.

Following are key practices and procedures implemented by the IT staff as routine Data Center operations:
Daily backups of HRMS system and data
Backups on demand in direct support of HR staff requirements
24/7 on-site hosting system and network monitoring
24/7 help desk support and monitoring
24/7 security staff
Strictly enforced security procedures
Photo ID required for building access
Sophisticated computerized access control system
Card key scan required for collocation space access
Video surveillance at all entrances and every aisle (90-day, on-site tape retention)
Locked racks and cabinets with local key management

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. USMC NAF HROs

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center; AAFES

☒ **Other Federal Agencies.**

Specify. Bureau of Labor and Statistics; Social Security Administration

☒ **State and Local Agencies.**

Specify. All 50 State Offices of Taxation

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Bank of America; Fidelity Investments; SEI; Aetna; Continential National American Group; AON Hewitt; HMOs: Health Net; Kaiser California; Kaiser Hawaii; Kaiser Mid-Atlantic; Anthem

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.

Refusal to provide required personal information would prevent an individual from obtaining employment with HQ Semper Fit & Exchange Services or with any other local installation MCCS activities.

(2) If "No," state the reason why individuals cannot object.

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.

Personal information collected is used only to support an individual's employment (i.e., pay, benefits, etc.).

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.	Paper copy provided and signed at time of hire.

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.