PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:
NAF Financial Management System Software as a Service (NAF FMS SaaS)

2. DOD COMPONENT NAME: Department of the Navy/United States Marine Corps

3. PIA APPROVAL DATE: 02/07/20

Marine Corps Manpower and Reserve Affairs (M&RA), Business and Support Services (MR)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public
- From Federal employees and/or Federal contractors
- From both members of the general public and Federal employees and/or Federal contractors
- Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System
- New Electronic Collection
- Existing DoD Information System
- Existing Electronic Collection
- Significantly Modified DoD Information System

The new Non-appropriated Fund Financial Management System Software as a Service (NAF FMS SaaS) will be an integrated accounting system that provides a means to manage and administer financial records related to general ledger, accounts payable, fixed assets, accounts receivable, and cash management. Additional functions will include inventory management, purchasing and procurement management, project costing, and a self-service portal for vendors/companies. Implementation of capabilities will be rolled-out in a phased approach.

Types of personal information include: individual's full name; personal identifier (Social Security Number (SSN), DoD ID number, Employer Identification Number (EIN), MCCS employee ID number, and MCCS assigned vendor/company ID number); vendor/company eligibility information; contact information (personal and work); military status and branch; rank and title information; payment and debt collection information; tender information; banking information; disbursing and accounting transaction data; supervisor's information; and purchase orders and invoices. A complete description and explanation are provided in the SORNs listed below.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII is collected for identification and verification of individuals and their contact information:
- for the creation of vendor/company contracts, purchase orders, invoices, recording their status, and for reporting required tax information;
- for verification of eligibility to conduct business with MCCS;
- for vendor/company payment;
- for data matching among systems;
- for a bad debt list to block patrons from future check tendering at a point-of-sale, as applicable;
- for the issuance of payments, collection of payments due, and recording their status;
- for the collection of outstanding debts, management of payments and outstanding balances, and recording any debt deduction or write-off;
- for the submission of required Internal Revenue Service (IRS) reporting for applicable contract payments and prizes;
- for employee remittance and reimbursement;
- for final wages payment to the employee's beneficiary, in the event of an employee's death;
- for creating an employee user profile and access to include transactional approval routing; and
- for analysis of financial transactions.

The intended use of the PII collected is for mission-related use and administrative use.

e. Do individuals have the opportunity to object to the collection of their PII? Yes ☑ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.
Vendors/companies may choose to provide business contact information and an employee identification number as opposed to personal contact information and a social security number.

The NAF FMS SaaS is not the original source of collection of all the personal information maintained. In the cases where the NAF FMS SaaS receives PII from other information systems, the individual(s) would have had the opportunity to object to the collection of their PII at that originating source (e.g., when making purchases by non-cash tender).

f. 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.

Providing information is considered consent. All information collected on the individual may be used for mission-related and administrative use without consent of the individual.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.  (Check as appropriate and provide the actual wording.)

☐ Privacy Act Statement  ☒ Privacy Advisory  ☐ Not Applicable

Information from the approved NAVMC 11787, “Response to the Marine Corps NAF Debt Collection Notice,” will be maintained in NAF FMS SaaS. NAVMC 11787 was approved after submission of the PIA. Data will be input by MCCS personnel, not the individuals. Below is the Privacy Act Statement on NAVMC 11787.

NAVMC 11787, Response to the Marine Corps NAF Debt Collection Notice
OMB No. 0703-0075 expiration date 10/31/2022
PRIVACY ACT STATEMENT
AUTHORITY: 10 U.S.C. 5013; 10 U.S.C. 5041; MCO P1700.27B W CH1; MCO 7010.19; E.O. 9397 (SSN), as amended; and SORN M07010-2.
PURPOSE: Information requested is used for the purpose of managing and administering Marine Corps Nonappropriated Fund (NAF) delinquent debt collections, as applicable.
ROUTINE USES: Information will be accessed by Marine Corps Community Services authorized personnel with a need-to-know to meet the purpose. Information may be disclosed to the U.S. Department of Treasury for centralized administrative or salary offset and to credit card processors, banks, and other financial institutions to process payments. A complete list and explanation of applicable Routine Uses is accessible at https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/NavyUSMC-Article-List/.
DISCLOSURE: Voluntary; however, failure to provide the requested information may result in automatic submission to the Treasury Offset Program to withhold or reduce Federal payment(s) due to the respondent to satisfy the debt.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?  (Check all that apply)

☒ Within the DoD Component
☐ Other DoD Components
☒ Other Federal Agencies
☐ State and Local Agencies

Specify.

Specify.

Specify.

Specify.

Specify.

Specify.

Specify.

Shared Services Center; Business Intelligence (Cognos); NAF Enterprise Contract Management (ECM) system; NAF Retail Management System (RMS); NAF Human Resource Management System (HRMS); MCCS bad debt database; and Secure File Transfer Protocol.

Defense Finance and Accounting Service (DFAS) and Army & Air Force Exchange Service (AAFES)

Internal Revenue Service
MCCS NAF procurement is used for the NAF FMS SaaS. NAF contracts are not subject to the Federal Acquisition Regulation (FAR) or DoD FAR Supplements. Privacy safeguards for NAF FMS SaaS falls under the Oracle Cloud Services NASA SEWP V Supplemental Terms and Conditions.

Creoal Consulting, LLC
Privacy safeguard language in the contract includes the NAF equivalent to FARs 52.224–1 Privacy Act Notification; 52.224–2 Privacy Act; and 39.105 Privacy. In addition, the contractor shall comply with maintaining compliance with:
- Contractor personnel that will work longer than one month on the Contractor’s project under this contract will require a Common Access Card (CAC) issued by the Department of Defense.
- Compliance with the latest version of the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS), as required.
- Major credit card brand (Visa, MasterCard, Discover, and American Express) Service Provider requirements, as required.
- DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT), as required.
- Privacy Act and OMB requirements based on an augmented set of moderate impact and privacy controls listed in NIST 800-53.
- MCCS internal requirements for review and written approval of all hardware, software, and services by the MCCS Cybersecurity and Compliance Office, prior to purchase, as well as any additional communications (ports, protocols, and services) external to the MCCS Network boundary.

Ernst & Young (EY), LLC
Privacy safeguard language in the contract includes the NAF equivalent to FAR 52.224–2 as well as the following:
- Privacy Act Data shall not be stored on any mobile storage device i.e., laptops, thumb drives, portable hard drives, etc.
- If transmitting Privacy Act Data, files shall be encrypted, password protected, or sent via secure FTP.
- Contractor shall ensure that all Personally Identifiable Information (PII) obtained under this contract is maintained and safeguarded as required under the Privacy Act of 1974 and the Department of Defense implementing regulations. Contractor must complete the PII training and provide certificate of completion to the MR Contracting Officer. The on-line training may be accessed at http://iase.disa.mil/eta/pii/pii_module/index.html.

Banking institutions to include Bank of America
i. **Source of the PII collected is:** (Check all that apply and list all information systems if applicable)

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [X] Databases
- [X] Commercial Systems

Individuals would be the source of information provided on NAVMC 11787.

MCCS finance offices; Shared Services Center; NAF HRMS; NAF ECM; MCCS procurement; commercial providers to include Bank of America Merchant Services; existing DoD information systems to include DFAS and AAFES; databases to include records of outstanding indebtedness to MCCS submitted from Marine Corps installations and the MCCS bad debt database; and self-service portal for vendors or businesses.

j. **How will the information be collected?** (Check all that apply and list all Official Form Numbers if applicable)

- [X] E-mail
- [X] Face-to-Face Contact
- [X] Fax
- [X] Information Sharing - System to System
- [X] Other (If Other, enter the information in the box below)

System-to-system transfer is via a secure file gateway connection. Website includes Oracle self-service portal for vendors/companies.


k. **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 must be consistent.

- [X] Yes
- [ ] No

If "Yes," enter SORN System Identifier **NM01700-1, NM04060-1, NM07010-1, N**

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or [http://dpcld.defense.gov/Privacy/SORNs/](http://dpcld.defense.gov/Privacy/SORNs/)

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. **What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

1. NARA Job Number or General Records Schedule Authority. **GRS 1.1 item 11**

2. If pending, provide the date the SF-115 was submitted to NARA.

3. Retention Instructions.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.

(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN NM01700-1, DON General Morale, Welfare, and Recreation Records (February 12, 2008, 73 FR 8035), authorities:


SORN NM04060-1, Navy and Marine Corps Exchange Sales Control and Security Files (April 30, 2008, 73 FR 23450), authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN), as amended.

SORN NM07010-1, DON Non-Appropriated Funds Standard Payroll System (June 16, 2014, 79 FR 34305), authorities:

10 U.S.C. 5013, Secretary of the Navy; CNICINST-7000.3, Accounting Procedures for Non-Appropriated Funds; and E.O. 9397 (SSN), as amended.

SORN NM01754-3, DON Child and Youth Program (May 27, 2010, 75 FR 29728), authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; DoD Instruction 6060.2, Child Development Programs; DoD Instruction 6060.3, School Age Care Program; DoD Instruction 6060.4, Youth Programs; OPNAV Instruction 1700.9 series, Child and Youth Programs; MCO 1710.30, Marine Corps Child and Youth Programs (CYP); and E.O. 9397 (SSN), as amended.

SORN N04066-4, Navy Lodge Records (April 30, 2008, 73 FR 23448), authorities:

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


n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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  ☐ No  ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.

(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."

(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

In accordance with OMB Memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act," dated April 7, 2010, the vendor information collected is not subject to the PRA as it is necessary for the selection, payment, or delivery of an item or service. In the cases where the NAF FMS SaaS receives information from other information systems, OMB requirements reside with the originating source of the information collection.