PRIVACY IMPACT ASSESSMENT (PIA)

For the

Accounting and Information Management System (AIMS)
Department of the Navy - CNIC

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: 6884 DITPR DON ID: 21029

☐ **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: 007-000006632

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 NM01700-1, N07200-1, and N05230-1

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 ID: NM01700-1

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
26 U.S.C. 6041
BUPERS Instruction 1710.11C, Operations of Morale, Welfare and Recreation Programs 2003
MCOP 1700.27, Marine Corps, Morale, Welfare and Recreation Policy Manual, Ch 1
NAVSO P-3520, Financial Management Policies and Procedures for Morale, Welfare and Recreation Programs
DoD 6025-18R, DoD Health Information Privacy Regulations
E.O. 9397 (SSN), as amended.

SORN ID: N07200-1

10 U.S.C. 5013, Secretary of the Navy
31 FR 285.11, Administrative Wage Garnishment
Federal Claims Collection Act of 1966 (Pub.L. 89-508) and Debt Collection Act of 1982 (Pub.L. 97-365)
E.O. 9397 (SSN), as amended.

SORN ID: N05230-1

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
CNICINST 5230.1, Total Workforce Management Services
OPNAVINT 3440.17, Navy Installation Emergency Management Program
DoD 6025-18R, DoD Health Information Privacy Regulations
E.O. 9397 (SSN), as amended

FINANCIAL MANAGEMENT POLICY MANUAL
NAVSO P-1000 Rev through Change 67

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 Accounting and Information Management System (AIMS) is the named system being utilized within Commander Navy Installations Command (CNIC) N9 to umbrella ALL the required applications that support the core business functions for the various divisions. AIMS is a Non-Appropriated Fund (NAF) system that allows the applications to run collectively and independently to gather and transmit Accounting & Reporting data, Planning information, Budgeting data, Inventory Management data as well as Personnel & Benefits Administration into one major application - SAP.

There are however numerous other applications such as Kronos Workforce Central, TeleTime, Micros, Recreational Tracking (RECTRAC), and Epitome Property Management System (PMS) that are supporting the CNIC N9 core business functions: MWR and NGIS, Civilian NAFIs (cafeterias, recreation funds), Fisher House Funds, Navy Retirement Homes, War Fighter Housing and Navy Flying Clubs that provide financial accounting and reporting, procurement, and human resources management within the AIMS environment.

Personnel Information Collected within the System: Name, SSN, Truncated SSN, Driver's License, other ID Number: DoD ID Number and Employee number;, Citizenship, Legal Status, Gender, Race/Ethnicity, Birthdate, Personal Cell Phone Number, Home Phone Number, Personnel Email address, mailing/Home address, security clearance, Spouse and Child Information: Name, SSN, Date of Birth (DOB), Address if needed; Martial Status, Medical information: planned enrolled, medical history, medications taken, and injury status; Disability information: Handicap status, if they're on disability; employment information: Location, Pay Plan series, Grade, Position, Title, Employment status(full time, part time or flex); Emergency contact: Name, Address, Telephone number; and Education information: Highest level achieved prior to start of employment and any additional while working for command; Financial information: Pay, Bank Information, Tax Deductions; and other: Veteran Status

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

Privacy risks are: (1) unauthorized access to the servers, (2) disclosure of PII/PCI to Individuals without a valid need-to-know, and (3) accidental disclosures.

1.) AIMS is on a commercial, private Multi Protocol Label Switching (MPLS) network. Any traffic allowed into the MPLS network must traverse the Firewall and Intrusion Prevention/Detection Systems, which are managed by Verizon Business. Traffic into the MPLS environment is encrypted SSL/TLS or IPSEC traffic. Aims uses role-based authorization to restrict access to systems and data by a user's job responsibilities

2.) The privacy risks include computer hackers, disgruntled employees and state-sponsored information warfare. All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that AIMS with its collection of PII/PCI, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. All systems are vulnerable to “insider threats”. AIMS administrators are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to AIMS. These individuals have gone through extensive background and employment investigations.

Mitigation:
The following controls are used to mitigate the risks:
a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. Since the server and data reside within an Navy establishment, the strict security measures set by the establishment are always followed.

3.) The risk of accidental disclosure of PII/PCI is addressed through an active management program. Aggressive actions for Improvement are continuously taken. Individual privacy is protected by requiring personnel to take extensive annual privacy trainings. PCI assessments are completed annually. Privacy trainings takes place to address privacy risks and refresher privacy trainings are conducted throughout the year.

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. CNIC Total Workforce Management Services (TWMS) Administrators

☒ **Other DoD Components.**

Specify. U.S. Air Force Data Center San Antonio, TX

☒ **Other Federal Agencies.**

Specify. Department of Treasury, ADP Payroll Processors

☐ **State and Local Agencies.**

Specify.

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

Specify. Immersion and Softbrands; Contracts contain language (FAR clauses) which requires the contractor to comply with the Privacy Act of 1974, as amended. Contractors have access to privacy data and are bound to the Privacy Act by the terms of the contract. They agree to abide by the Privacy Act of 1974.

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

Specify. Bank of America

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.

Data is collected directly from staff members (individuals) via direct access to the application, and they have the ability to object and/or question the collection of PII at that time. Data is also retrieved from information systems rather than directly from individuals, and in those cases individuals are not provided either a Privacy Act Statement or a Privacy Advisory from the system. However, individuals implicitly consent to capture and use of that information at the time of employment, at which time they are provided a Privacy Advisory.

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

N/A

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.

Data is collected directly from staff members (individuals) via direct access to the application, and they have the ability to object and/or question the collection of PII at that time. Data is also retrieved from information systems rather than directly from individuals, and in those cases individuals are not provided either a Privacy Act Statement or a Privacy Advisory from the system. However, individuals implicitly consent to capture and use of that information at the time of employment, at which time they are provided a Privacy Advisory.

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

N/A

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.	There are Privacy Act Statement on the web sites. There are Privacy Act Statement on applicable forms. Verbally stated. Privacy Act Statements are posted in some locations.

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.