



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

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
- 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

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

Package submitted. (Pending)

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 N07200-1 (Navy Morale, Welfare, and Recreation Debtors List (January 29, 2007, 72 FR 3983)) authorities:

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); and E.O. 9397 (SSN).

- To maintain an automated tracking and accounting system for individuals indebted to the Department of the Navy’s Morale, Welfare and Recreation (MWR) facilities for the purpose of collecting debts.

- Records in this system are subject to use in approved computer matching programs authorized under the Privacy Act of 1974, as amended, for debt collection purposes.

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

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; and E.O. 9397

(SSN) (As amended).

- To provide a means of paying, recording, accounting, reporting, and controlling expenditures and merchandise inventories associated with MWR programs, activities, and events to include raffles, Monte Carlo, bingo prizes, and gaming machines.

- To provide on-base emergency personnel with medical information regarding the emergency.

SORN ID 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).

- 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 withholdings 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.

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

- Provides a compendium of the requirements, principles, standards, systems, procedures and practices governing financial management as well as a discussion of organizational and appropriation responsibility for funding of particular types of costs and functions.

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: Name, SSN, Truncated SSN, Driver's License, other ID Number, Citizenship, Legal Status, Gender, Race/Ethnicity, Birthdate, Personal Cell Phone Number, Home Phone Number, Personnel Email address, mailing/Home address, security clearance, Spouse Information, Martial Status, Child information, Medical information, Disability information, employment information, Emergency contact, and Education information.

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

AIMS employs several measures to address privacy risks and protect PII/PCI. AIMS uses role based authorizations to restrict access to systems and data by a users job responsibility and need-to-know. Authorized users must sign a Privileged users agreement . This method ensures only authorized users, with a need to know, are able to access the system data. This allows system administrators to accurately track user activity and determine if users are uploading unauthorized PII/PCI. The information is used for official use only and using role based access restricts use by unauthorized users of the system.

Measures include firewalls, TLS (https), SFTP, intrusion detection, and port security.

AIMS currently employs 128-bit/256-bit encryption via Transport Layer Security (TLS) to protect the transmission of personal information. AIMS does not contain any classified information. The primary measure to protect the information stored in AIMS resides in the underlying operating system security subsystem. If a server crash were to occur, a full-time database administrator will manage the server logs and identify potential problems or issues with the server. The database administrator has in place a back up and restore process that allows the application to be re-installed and configured.

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.

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.

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.

-Data collected is essential for Human Resource staff members in the hiring process of employees, includes CAC ID, Payroll and access to the IT Network.
-To provide health and personal information to an off-base medical treatment facility should a member be taken there for treatment.
-To the Internal Revenue Service to report all monies and items of merchandise paid to winners of games whose one-time winnings are \$1,200 or more.
-To the Internal Revenue Service to record wages earned, tax withheld and social security information.
-To state revenue departments to credit employee's state withholding.
-To state employment agencies which require wage information to determine eligibility for unemployment compensation benefits of former employees.
-To city revenue departments of appropriate cities to credit employees for city tax withheld.
-To a debt collection agency for the purpose of collection services to recover indebtedness owed to the Department of the Navy.
-To the Internal Revenue Service (IRS) to obtain the mailing address of a taxpayer for the purpose of locating such taxpayer to collect or to compromise a Federal claim by Navy against the taxpayer pursuant to 26 U.S.C. 6103(m)(2) and in accordance with 31 U.S.C. 3711, 3217, and 3718.
-To any State and local governmental agency that employs the services of others and that pays their wages or salaries, where the employee owes a delinquent non-tax debt to the United States for the purpose of garnishment.

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.

-Data collected is essential for Human Resource staff members in the hiring process of employees, includes CAC ID, Payroll and access to the IT Network.
-To provide health and personal information to an off-base medical treatment facility should a member be taken there for treatment.
-To the Internal Revenue Service to report all monies and items of merchandise paid to winners of games whose one-time winnings are \$1,200 or more.
-To the Internal Revenue Service to record wages earned, tax withheld and social security information.
-To state revenue departments to credit employee's state withholding.
-To state employment agencies which require wage information to determine eligibility for unemployment compensation benefits of former employees.
-To city revenue departments of appropriate cities to credit employees for city tax withheld.
-To a debt collection agency for the purpose of collection services to recover indebtedness owed to the Department of the Navy.
-To the Internal Revenue Service (IRS) to obtain the mailing address of a taxpayer for the purpose of locating such taxpayer to collect or to compromise a Federal claim by Navy against the taxpayer pursuant to 26 U.S.C. 6103(m)(2) and in accordance with 31 U.S.C. 3711, 3217, and 3718.

-To any State and local governmental agency that employs the services of others and that pays their wages or salaries, where the employee owes a delinquent non-tax debt to the United States for the purpose of garnishment.

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.

The PII is collected when a new employee is hired. The new employee must fill out forms for Payroll, Health Benefits for them and their family members, Retirement and TSP. This information is input to SAP by HR staff members. When a new employee is hired they are provided a PAS at the time they check onboard.

PII and Card Holder Data (CHD) is also collected when customers register to stay at the Navy Gateway Inns & Suites (NGIS) or Navy Getaways - RV Parks & Cottages. There is no PAS associated with the collection of customer's information when they register. The Customers register online at <http://www.dodlodging.net/> or at the Front Desks. The CHD is collected through the Point of Sale (POS) and is stored in the Millington and San Antonio Data Centers.

Internal Revenue Forms W2-G and 5754 for the IRS are collected when an Individual wins Gambling Winnings and Statement by Person(s) Receiving Gambling Winnings, or items of merchandise worth \$1200 or more, respectively. No, there is no PAS associated with individuals gambling winnings or items of merchandise totaling \$1200 or more in one winning. This information is collected and inputted into SAP and is kept on file for two years. At the end of the year, the Individuals and IRS will receive a 1099.

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.