PRIVACY IMPACT ASSESSMENT (PIA)

For the

TOTAL WORKFORCE MANAGEMENT SERVICES (TWMS)
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: 6976 DITPR DON ID: 21023
- ☐ **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: 007-000001569

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 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 N/A

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:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
CNICINST 5230.1 Total Workforce Management Services
OPNAVINST 3440.17 Navy Installation Emergency Management Program
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.

TWMS primary function is to pull information from official systems of record and combine this data into one comprehensive database warehouse and web application, which allows management, supervisors, admin support personnel, and HQ personnel with appropriate permissions to access both personnel and manpower information for their Total Workforce. Employees using their DoD issued Public Key Infrastructure (PKI) certificates can access their own record and information at any time without restriction. Typical uses of the data include generation of reports for submission to higher authority, demographics, workforce metrics/ structure/alignment, workflow processes such as SF-182 processing/Telework Agreement documentation/ System Authorization Access Request (SAAR) management, daily personnel accountability, contingency operations in the event of a natural or man-made disaster, historical trend analysis, employee human resources, workforce resource management, billet to personnel alignment, performance management, special/training programs tracking, management and certification, as well as locator services. The application is roles and permissions based, and is secured via use of web encryption, PKI certifications, user ID, and DoD Common Access Card (CAC) authentication. 90% of the data in TWMS is provided from official program of record interfaces, the remaining 10% is entered and maintained by local commands and is unique to their organization.

PII collected includes Name, other name used, SSN, DOB, place of birth, gender, mailing/home address and contact information: personal cell/home telephone number, personal email address; citizenship, religious preference, marital status, Spouse & Child Information: age, co-location indicator to prepare emergency evacuation orders and morale welfare and recreation (MWR) demographic accounting; military records: awards, salary and leave data, security clearance, nationality, race; emergency contact, other ID number: DoD EDIPI (Electronic Data Interchange Personal Identifier); law enforcement information such as controlled access to badge identification numbers, weapon assignment status, and other law enforcement/investigative sensitive/privileged information; medical information: limited to flu survey data voluntarily provided by individuals and also medical information collected in support of the Wounded Warrior Safe Harbor Program; employment information: work history, assigned billet and asset information, qualification information, and performance; education information: education, skills/certification/competencies required and acquired; disability information: type of disability; and as provided by the official programs of record or voluntarily by the employee.

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

Risks include unauthorized disclosure by personnel with access, and network intrusion. Intrusion is mitigated by the encryption of data, location behind the Navy and Marine Corps Intranet (NMCI) fire wall, and requiring DOD PKI authentication as well as User ID and strong password authentication. Unauthorized disclosure is mitigated by the requirement of all personnel with access to complete annually the DOD Privacy Act (PII) training and DOD Information Assurance (IA) Awareness training, and automatic suspension of user accounts when personnel actions reassigning users are processed.
Access to data is multi-tiered and based on a need to know, and is managed by a designated command representative knowledgeable in the area of that command's total workforce. The first tier of a user account is profile based, which limits the user to specific employee types and/or data, such as training data, or muster/ accountability data, or position management data. Users in a specific profile cannot view data outside of that profile's restriction. The second tier further restricts access by use of permissions, which allow a user specific access to application functions, such as linking billets to employees, viewing restricted PII fields such as SSN and DOB, viewing SF-50 history, preparing SF-182's, and management of the IA workforce. Specific role based permissions may be viewed in the access level matrix located on the documentation page on the application web site. Physical access to terminals, terminal rooms, buildings and activities' grounds are controlled by locked terminals and rooms, guards, personnel screening and visitor registers. All data is kept in a certified data facility. At no time is data removed from the secure hosting environment and access to data is only to those employees with a direct functional need. Use of the DOD Common Access Card (CAC) as well as use of profiles and permissions assists in

assuring only appropriate personnel have access to data.

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. NETC-NTMPS reverse interface, SPAWAR-CIVPERS WEBSERVICE, , NAVSEA/NAVAIR-ERP, NCIS-WEBSERVICE, SPECWARCOM-WEBSERVICE, CNIC Enterprise Gateway/iShore, OCHR-DCPDS reverse interface

☐ **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.

Individuals can object to the collection of PII by following the procedures outlined in N05230-1 or by declining to provide the information unless specified as mandatory for "key", "emergency", or "critical" essential personnel as designated in OPNAVINST 3440.17. Failure to either provide or verify the accuracy of TWMS data may result in employees or their emergency points of contact not being contacted in the event of recall, mobilization, emergencies, or other work or personal planning outcomes.

Information from the programs of record is subject to objection at the source system. Collection of information directly from the individual is voluntary.

(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.

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

Collected data is utilized for mission essential reporting.

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.

TWMS Log in page contains Privacy Act Statement that informs the user of the authority, purpose, routine uses for the collection of PII and a disclosure statement regarding the collection mandate status and possible consequences of non provision.

Statement reads:

PRIVACY ACT STATEMENT

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

Purpose: To collect personal and work-related information necessary to manage, supervise, and administer all aspects of Department of the Navy (DON) programs for military, civilian, Non-Appropriated Fund (NAF) and contract members of the workforce.

Routine Uses: To assist command personnel on such matters as, but not limited to, preparing recall rosters and locators; maintaining accurate phone directories and manpower documents; contacting appropriate personnel in emergencies or during force mobilization; training the workforce; identifying routine and special work assignments; determining clearance for access control; assisting in

manpower research studies; controlling the budget, travel expenditures, manpower and grades; maintaining statistics for employment; projection of retirement losses; labor costing; safety monitor reporting; tracking and reporting on the Navy's Information Assurance (IA) workforce, and similar administrative uses requiring personnel data. Any disclosures would be For Official Use Only as information is "close-hold" and shared with only those with an official "need-to-know". Some data, such as work location, communications and functional areas are generally available to the entire workforce. Access to remaining data is generally restricted to tiers of civilian and military supervisors ranging from immediate workplace supervisors to Site and Program Managers, Program Directors, and Military Commanders and their immediate staff. Administrative personnel will have access for purposes of maintaining the intranet and TWMS databases.".

Disclosure: Mandatory for Military. Mandatory for civilian, NAF, and contract personnel who have been designated by their organizations as "key", "emergency" or "critical" essential personnel. Mandatory for civilian, NAF, and contract personnel in positions that have been identified as part of the Navy's IA workforce in accordance with DOD 8570.01-M. Voluntary for all other civilian, NAF and contract personnel. In many instances, requested data (e.g., social security numbers and security clearances) may be available from other authorized databases. Failure by any workforce member to either provide or verify the accuracy of TWMS data may result in employees or their emergency points of contact (POCs) not being contacted in the event of recall, mobilization, emergencies, or other work or personal planning outcomes.
TWMS SORN #N05230-1

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.