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:
TOTAL WORKFORCE MANAGEMENT SERVICES (TWMS)

2. DOD COMPONENT NAME: Department of the Navy

3. PIA APPROVAL DATE: 05/11/20

Commander, Navy Installations Command (CNIC)

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)

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

b. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Total Workforce Management Services (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, military funeral honors request processing and tracking, 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 and Child Information, age, location indicator to prepare emergency evacuation orders and morale welfare and recreation (MWR) demographic accounting, military records: 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, skills/competencies required and acquired, disability information, type of disability, and as provided by official programs of record or voluntarily by the employee.

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)

Data is required to identify, verify, and authenticate employee personnel and position information relevant to total workforce management; cross reference and data match across programs of record for resolution of disparate record keys and consolidation of record data.

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.
Individuals can object to the collection of PII by following the procedures outlined in N05230-1A, or by declining to provide the information unless specified as mandatory for "key", "emergency", or "critical" essential personnel as designated in OPNAVINST 3440.17(series). 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 a 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.

f. Do individuals have the opportunity to consent to the specific uses of their PII?  [ ] Yes  [x] 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.

Consent is assumed when information is provided.

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.)

[x] Privacy Act Statement  [ ] Privacy Advisory  [ ] Not Applicable

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), N05230-1.

Purpose: To collect personal and work-related information necessary to manage, supervise, and administer all aspects of DON programs for military, civilian, NAFI 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 POCs not being contacted in the event of recall, mobilization, emergencies, or other work or personal planning outcomes.

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  Specify.

[ ] Other DoD Components  Specify.

[ ] Other Federal Agencies  Specify.

[ ] State and Local Agencies  Specify.

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

[ ] Other (e.g., commercial providers, colleges).  Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

NETC-NTMPS reverse interface, NAVSEA/NAVAIR-ERP, NCIS-Webservice, NAVFAC-webservice, DOD-CMS Webservice, CNIC Enterprise Gateway/G2, OCHR-DCPDS Reverse interface

Specify.
Individuals

Existing DoD Information Systems

Other Federal Information Systems

AEM Designer

DD FORM 2930, JUN 2017

PREVIOUS EDITION IS OBSOLETE.
(3) Retention Instructions.

Retire to nearest FRC when 4 years old. Destroy when 20 years old.

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 N05230-1, Total Workforce Management Services (TWMS) (October 20, 2010, 75 FR 64715) (revision in progress) authorities: |
| 10 U.S.C. 5013, Secretary of the Navy |
| 10 U.S.C. 5041, Headquarters, Marine Corps |
| CNICINST 5230.1A Total Workforce Management Services |
| OPNAVINST 3440.17 (series), Navy Installations Emergency Management Program |
| 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  X 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.

TWMS does not collect information from the public that requires an OMB Control Number