



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Trident Resource Management System (TRMS)
---

Department of the Navy - NAVSEA - PSNS
--

### **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

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 N01070-3 authorities:

10 U.S.C. 5013, Secretary of the Navy

42 U.S.C. 10606 as implemented by DoD Instruction 1030.1, Victim and Witness Assistance Procedures  
E.O. 9397 (SSN), as amended

SORN N05230-1 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.

TRMS manpower module coordinates all assigned officer, enlisted and civilian personnel with authorized billets/positions. It provides the ability to produce demographic reports; it is a recruitment tool and a tool for use for manpower/labor forecasting. In addition, TRMS provides critical input to the CRMMS system which provides timekeeping services for use by payroll, as well as LDS (labor distribution). TRMS is used to manage the command recall function. It is also used to check-in/checkout personnel and to manage civilian and military billets.

Description from DITPR DON: Trident Resource Management System (TRMS) is located at Puget Sound Naval Shipyard & Intermediate Maintenance Facility (PSNS & IMF) for the maintenance & planning purposes of Trident submarine & surface ships at Everett, Bangor, & PSNS. TRMS supports the production of the Intermediate Maintenance Facility (IMF) by automating them into a single menu system. Department heads, planners, administrative, quality assurance personnel & logistics personnel, input data & have ready access to command & technical documentation, manpower, training, qualifications, acquisition, financial/accounting, & support personnel, to perform their task & to fulfill requirements in meeting Trident SSBN (Ballistic Missile Submarines) strategic patrol schedules. All of the TRMS Data is kept in one centralized Database & can be used throughout the various TRMS programs. TRMS also tracks a variety of Military data including Career Counselor data, Physical Fitness data, Auxiliary Security Force data, & Leave data. TRMS provides data elements for IMF Logistic Data System (LDS) application database servers in support of Timekeeping Command Resource Management Module (CRMM), LDS Security Access, Supply, & Trident System production. Department Resource data is sent daily to the LDS Preprocessor module to keep Funding Documents Status current. A daily procedure allows LDS to add usernames & their access to the appropriate databases by reading TRMS data. The payroll program, CRMM, reads TRMS data each night to keep its personnel table accurate. Supports Navy Mandated/OPNAV 4000.57F LDS for Trident Maintenance. Contains critical VB & Web applications that provide functional, administrative, and Command support of Manpower, Training, Comptroller, Financial/Accounting, Safety, Security, Personnel, Trident Repair, Hazardous Materials, etc. It administers Navy Region Northwest applications essential for support of the LDS. Provides functional, administrative, & Command support of Manpower, Training, Comptroller, Financial/Accounting, Safety, Security, Personnel, Trident Repair, Hazardous Materials.

Personal Identifiable Information (PII) collected: Name, SSN, Badge Number, Gender, Race/Ethnicity, DOB, Personal Cell Phone, Home Phone, Home address, Spouse Information: name, age and gender; Marital Status, Child Information: number, age, and gender; Disability Information: special needs; Military Records: billet and rank; Emergency Contact, Education Information: high school and college level degrees; training courses, qualifications; and Other ID Number: Badge Number.

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

Potential privacy risks may result from inadvertent disclosure or hacking. Application is located on the PSNS&IMF network. The network is protected with required security standards per DoDD 8500.1 and DoDI 8500.2 and technical security features such as firewalls, IDP/IPS, access control and encryption.

**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.

Puget Sound Naval Shipyard Training Coordinators, Administrative Assistants, Supervisors, Manpower/Training Office personnel, Military Personnel Office.

**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.

PII is not collected directly from the individual. A digitally signed and encrypted e-mail is received in the Manpower Office from the local Human Resource Service Center (HRSC) office with attached data files used to upload into TRMS.

**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.

PII is not collected directly from the individual. A digitally signed and encrypted e-mail is received in the Manpower Office from the local HRSC office with attached data files used to upload into TRMS.

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

- |  |   |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other                 | <input checked="" type="checkbox"/> None  |

Describe each applicable format.

PII is not collected directly from the individual. A digitally signed and encrypted e-mail is received in the Manpower Office from the local HRSC office with attached data files used to upload into TRMS.

**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.**