



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Non-Tactical Data Processing Subsystem (NTDPS)
--

Department of the Navy - NAVSEA

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 Authorities:

5 U.S.C. 301, Departmental Regulations;
10 U.S.C 5013, Secretary of the Navy;
10 U.S.C. 620, Active-duty lists;
10 U.S.C. 617, Reports of Selection Boards; and
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.

To assist Navy officials and employees in the classification, qualification determinations, career development, education and training of Navy personnel to meet training allocations and requirements. The system will provide an automated process to support all non-tactical operations including maintenance, training, operations, supply, and administrative functions which are carried out on the submarine platform.

The types of PII collected include: Name, Other names used, SSN, Other ID Number: DoD ID Number, Other ID Number is selected by the afloat unit and not controlled by the Program Office; Citizenship, Gender, Birth Date, Security Clearance, Marital Status, Military Records: Home Telephone Number, Mailing/Home Address, Service Date, Reporting Date, CADD Date, Current Enlistment date, PR date, End of Active Obligated Service (EAOS) Date, EAOS Extension, Geographical Bachelor, Frocked, Supervisor ID, Bunk ID, Division Assignment, Status, Posting Date, Posting ID, Radiation Assessment Date, Previous Nuclear Experience, Next Assignment, Rate and Paygrade, Allowance Rate, Navy Enlistment Classification (NEC), and Advancement Date; and Emergency Contact: Name, best phone, address, e-mail for contact.

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

The chief risk to the collected PII is authorized disclosure, which can potentially result in loss of privacy or identity theft by malicious actors.

These risks are addressed through security controls implemented by the NTDPS application is within the Host IS and physical shipboard environment. Access to PII is regulated through structured, role-based logon permissions and passwords implemented at the system and application levels, and through tight physical access controls implemented by afloat platforms.

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.

PII is only used with the internal confines of the afloat platform (shipboard use only, no external transmission).

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.

Individuals are required to use NTDPS as part of the shipboard routine, and the PII must be entered to maintain a record of the training and personnel requirements specific to each sailor.

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.

Individuals are required to use NTDPS as part of the shipboard routine, and the uses of PII are required to fulfill the personnel documentation requirements set forth by the Navy and implemented by NTDPS. The PII is used to verify the identities of the individuals tracking their education and qualification requirements in accordance with Navy standards.

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

Describe each applicable format.

The user is required to acknowledge the a Privacy Advisory notice prior to logging on to the system. This notice states that the user is utilizing a DoD system, and their use of the system may be monitored. The user is required to explicitly acknowledge this warning prior to entering any credentials to access the system.

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.