



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Target Position Organizational Structure (TPOS)

Department of the Navy - NAVSEA - Naval Shipyards-PNS

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:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
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.

This application keeps track of all the Shipyard civilian positions and who is filling those positions as well as the organizational structure of the Shipyard. The Target Position Organization Structure (TPOS): (1) tracks core and non-core billets through the identification of position category codes (full time billet, established for the incumbent only, billets established in error, temporary billets, duplicate billets, billets slated for abolishment or downgrade when unencumbered, and special hires); (2) status codes are assigned for each category code (core, attrition, backfill for attrition, details in or out of a billet, DCPDS error, new billets for external hires, NAVSEA billets, obligated billets); (3) tracks BSC/BIIN numbers to individual authorized billets, which is not only mapped to the billet, it includes the name of the individual in that billet; (4) personnel use this program to track actual dates for temporary promotion/reassignments; (5) detail to duties are tracked (which HR will not process); (6) keeps track of apprentices (WSPP & WSAPR); (7) allows Departments to view positions/employees in their respective department; (8) identifies target grades and pay plans; (9) allows Management to see their respective organization structure and specific information above; (10) and supports the human capital metrics which are used by the Executive Steering Group (Government's version of a Board of Directors), Full Time Equivalent Board (Board that oversees the execution of Human Capital) and the Position Manager (oversees all position management). This program also allows the use of "notes" for any billet, which allows the administrators and Position Manager to enter data, for internal use only (High Grade Approvals, actual dates an employee separated who encumbered an "attrition" billet), etc. This program also maps the "typical charge code" which identifies the billet as either direct, overhead or quasi (direct and overhead), for labor charging profiles. This program allows the user to "run reports"; they can run a standard report or build one. The reports can also be exported to Excel, for other uses.

Personal information collected: name, Social Security Number, DoD ID Number/Badge Number, office phone, public key ID, network account information, office email address, position and pay grade, and organizational affiliation.

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

To prevent unauthorized access to the PII information, connections to the system are limited to those protected within the Portsmouth Naval Shipyard and/or NMCI firewall and trusted networks. Access to these networks is secured through the use of cryptographic logon using the Common Access Card and associated PKI certificates. Access to this specific system is further secured through the use of Access Control Lists based on supervisory determinations of need-to-know. All internal personnel who are given access to the network are required to have security investigations conducted to establish their trustworthiness, and generally have a Confidential or higher security clearance.

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.

TPOS does not collect PII directly from the individual.

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.

TPOS does not collect PII directly from the individual.

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.

TPOS does not collect PII directly from the individual.

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.