



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Portsmouth Naval Shipyard Occupational Accident And Illness Reporting System  
(POAIRS)

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.

Other authorities:

OPNAVINST 5100.23G, Navy Safety and Occupational Health Program Manual  
DoD 6025 18-R, DoD Health Information Privacy Regulation

**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.

The mission of the Portsmouth Naval Shipyard Occupational Accident and Illness Reporting System (POAIRS) is to provide an automated, online capability for supervisors to complete investigations of mishaps that result in occupational injuries and illnesses. Automated routing of investigations through the concurrence cycle is also provided by POAIRS. POAIRS also provides for email notifications of mishaps to the appropriate personnel. Mishap investigation is required by OPNAVINST 5100.23F. If POAIRS were not available, the Shipyard would have to resort to hardcopy forms and the regular mail system to achieve the required results. POAIRS allows the Shipyard to meet the OSHE 3-day reporting requirement.

POAIRS is an application tool that is used by the supervisors of Portsmouth Naval Shipyard to enter their interpretation of an injury or illness of one of their employees. When filling out the on line form they input the employee's badge number. The application looks this badge number up in the Supdesk data and prepopulates the form with the employee's work information. The supervisor acquires the medical information by interviewing the employee then inputs the data into the application.

Personal information collected includes: SUPDESK extracts information to fill out the form within POAIRS, information to include supervisors name, command name, hours worked per day and the following information below:

Employee name, badge number, DoD ID Number and Medical Information includes: date of injury / illness, where injury / illness took place, nature of injury / illness, disposition of injury / illness.

(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 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. Based on these protections, theft or other loss of personal information is unlikely.

**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.

Collection and use of PII is required to support work-related tasks. Employee personal information is obtained from SUPDESK not directly from the individual. Medical information is obtained through interview and manually entered by staff.

**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.

Collection and use of PII is required to support work-related tasks. Employee personal information is obtained from SUPDESK not directly from the individual. Medical information is obtained through interview

and manually entered by staff.

**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.

Collection and use of PII is required to support work-related tasks. Employee personal information is obtained from SUPDESK not directly from the individual. Medical information is obtained through interview and manually entered by staff.

**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.