



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Leaders to Sea Data Base

U. S. Navy - Chief of Naval Information

### **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
- New Electronic Collection
- Existing DoD Information System
- Existing Electronic Collection
- Significantly Modified DoD Information System

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.

10 U.S.C. 5013, Secretary of the Navy  
DoD Instruction 5400.13 Public Affairs (PA) Operations  
OPNAV Instruction 5726.8 OUTREACH: AMERICA'S NAVY

**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 purpose of this DoD information system is to gather information about individuals who want to embark on Navy vessels. A Navy public affairs officer will review this information to determine if the person qualifies for an embarkment.

The types of personal information collected by this system include: Name, Date and Place of Birth, Home Address, Home Telephone Number and Personal Cell Telephone Numbers, Personal Email, Gender, Medical Information (consisting of current medications and dosages; medical alert tag status and reason; existence of medical conditions or history such as asthma, diabetes, stroke, etc.; and consent to treatment), Emergency Contact, Food Restrictions, and Occupation.

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

Identity theft is a privacy risk if personal information is mishandled. This risk has been mitigated through administrative, technical, and physical safeguards.

Administrative, physical, and technical safeguards employed by the program are commensurate with the sensitivity of personal data to ensure preservation of integrity and to preclude unauthorized use/disclosure. Access is limited to those individuals who require the records in performance of their official duties. Access is further restricted by the use of passwords which are changed periodically. Physical entry is restricted by the use of locks, guards, and administrative procedures.

Administrative: Access to the system will be controlled through a secure web login interface. Designated personnel will only have access to particular areas of site that have been deemed necessary for the individual to perform his or her duties. Administrators will have access to all system records.

Physical: All personnel entering the computer room must have appropriate identification. Visitors to the room are always escorted. The computer room is a restricted area and access is permitted to only authorized personnel only. Physical entry is restricted by the use of locks and administrative procedures. Servers and workstations require privileged authentication and access is limited to approved administrators.

Technical: Data is stored on a secure database server. An end user, using their web browser, will pass through the firewall to the web server. This connection between the end user and the web server is a secure encrypted SSL session. The web server provides the interface with the database server that processes the transaction and passes the data back to the end user's browser.

**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.

Individuals will have the opportunity to object to the collection of their PII by electing not to enter the requested information. If the individual does object they will not be considered for an embark.

(2) If "No," state the reason why individuals cannot object.

**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.

Individuals will check a block to indicate consent. The PII is necessary to determine if the person qualifies for an embark.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

**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.

Format: Web site banner across the top of the web form.

Authority to request this information is derived from 10 U.S.C. 5013, Executive Order 9397 (SSN) as amended, and departmental regulations. The principal purpose of the information requested is to facilitate embark on a U.S. Navy surface ship or submarine, including notification of next of kin in the event of death or serious injury, and to permit transmission of public affairs information from the Navy to the individual concerned. Completion of the information is completely voluntary; failure to provide required information may result in denial of embark request.

**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.**