



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

OPNAV Headquarter Web (HQWeb)
-------------------------------

Department of the Navy - CNO-OPNAV
------------------------------------

### **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.

10 U.S.C. 5013, Secretary of the Navy  
DoD 8500.2, Information Assurance (IA) Implementation  
SECNAVINST 5239.3B, Department of the Navy Information Assurance Policy

**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.

Personal data is provided by the user for the purpose of authentication, authorization (for HQWeb and all subsystems), recall and accounting in cases of emergency, staff collaboration and coordination and to comply with SECNAVINST 5239.3B. (Controlling Access by Foreign Nationals).

Individual information to include: title, full name, current home address, home phone number, cell phone number, e-mail addresses, rank/grade, date of rank, nationality, brief biography, spouse's name, child(ren)'s name(s), and emergency contact name and phone number.

Work related information to include: Current supervisor's name, date checked in, last command, next command, office title, office address, office room number, office phone number, office DSN, office fax number, office e-mail address; office of primary responsibility, position title, organization code, office designator, clearance, clearance adjudication date, competencies, secondary phone number, area of responsibility, area of interest, End of Active Obligated Service, reporting to position code, UIC, and billet information.

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

Privacy risks exist with the collecting, transmitting and storing of PII information. Annual PII training is required by all OPNAV Staff so they are educated on the handling of PII prior to entering into HQWeb. Once the information is entered into the system the PII is encrypted and can only be accessed via the web-based HQWeb interface with an administrator or command manager account that is authorized to view. The HQWeb system is CAC enabled with the PII further protected by groups that limit access to command managers and specified individuals on a need to know basis. Command managers only have the ability to see contact information for those people in their command directory. Access to other command directories is not permitted.

Non electronic records are destroyed as per Navy records management policies outlined in SECNAVINST 5210.8D.

All information changes, additions and deletions are fully audited within the application. Information on what was changed by whom and when is all catalogued and reviewed on a routine basis. Access to information is logged via server traffic logs and is routinely monitored for inappropriate usage.

Privacy risks are low. Only authorized personnel have access to the recall data collected. Authorized personnel are authenticated to the system via DOD PKI certificates.

**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.

OPNAV only

**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.

All PII is collected directly from the user via a user interface in HQWeb. The user has the option not to provide any or all information; however, failure to provide the required information may result in access being denied to HQWeb and all subsystems.

(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.

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

Information collected is to meet administrative and information security requirements.

**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.

**PRIVACY ACT STATEMENT**

**AUTHORITY:**

SORN # N05000-1

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

DoD 8500.2, Information Assurance (IA) Implementation

SECNAVINST 5239.3B, Department of the Navy Information Assurance Policy

**PURPOSE:** HQWeb is a system of systems. It provides information for staff collaboration, to include flag officers and retired flag officers, internal and external staff coordination for the OPNAV staff, and other web services in support of staff functions to notify personnel of office closings; locate personnel and/or next of kin in case of emergency; or recall personnel as necessary.

**ROUTINE USES:** Supervisory personnel will have access to information concerning their employees. Administrative/web personnel will have access for purposes of maintaining the database.

**DISCLOSURE:** Voluntary. However, failure to provide information may result in our ability to contact you or your next of kin in an emergency; or inability to provide you notice of an office closing; or inability to grant access.

---

**SECURITY STATEMENT**

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.

**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.**