



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Reserve Homeport (NRH)

Department of the Navy (DON) - NAVRESFOR
--

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, Department Regulations
E.O. 9397 (SSN), as amended

Other Authorities:

10 U.S.C. 5013, Department of the Navy
10 U.S.C. Subtitle E, Reserve Components
1007, Administration of Reserve Components
BUPERS Instruction 1001.39F, Administration Procedures for Navy Personnel
OPNAV Instruction 100.16K, Navy Total Force Manpower Policies and Procedures

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.

Navy Reserve Homeport (NRH) is a centralized web publishing system for the Navy Reserve which allows subordinate commands from across the country to post and update information to their web pages. The system is comprised of a publicly available site for the PAO and a CAC enabled private site for FOUO subject matter. PII such as Social Security Numbers (SSN) are not collected/stored/posted on the public side. Access to the private side is restricted to DoD members with a valid/current CAC and permissions are managed by NAVRESFORCOM Administrators. PII is used for internal government operations. Most of the data is PII in NRH Private is stored information from other authoritative, legacy systems. T This PII data is protected and not accessible to NRH users, but used in internal administrative work flows and programs. Selected Reserve personnel may voluntarily provide their personal phone and e-mail addresses, due to their unique status.

PII collected includes: name, Social Security Number (full and truncated), DoD ID Number, citizenship, gender, date of birth, mailing/home address, security clearance, marital status, unit, rank, education information: education level, major/specialty code, and high school diploma/GED, years of education; personal phone numbers (home and mobile), personal e-mail addresses, and general contact information

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

The risks of PII spillage and unauthorized access are mitigated via training, policies, and technical access controls. Access to these sensitive databases is limited to trained and specifically authorized system administrators and site collection administrators with the appropriate security clearance.

Active Directory (AD) and Forefront Identity Management (FIM) assist our administrators manage access for all users.

Existing PII data from the Navy Reserve Data Warehouse - Decision Support System (NRDW - DSS), DITPR ID: 4934, DITPR DON ID: 20931, is also referenced by the system to filter and route requests for internal processes. This data is not stored or accessible by users.

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.

The contractor shall have an operational security program in strict compliance with the National Industrial Security Program Operating Manual (Department of Defense (DoD) 5220.22-M) and Space and Naval Warfare Systems Center, Atlantic (SSCA) security directives at the time of award. Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted.

If contractor personnel require access to any Navy IT systems or resources at SSCA (directly or indirectly), all contractor personnel shall be required to complete the mandatory annual IA training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified Contracting Officer's Representative (COR).

The contractor shall demonstrate expertise in supporting and complying with DoN and DoD enterprise initiatives that include Personally Identifiable Information (PII).

The Contractor shall conform to the provisions of DOD 5220.22M, SECNAVINST 5510.30, and the Privacy Act of 1974.

Contractor personnel shall sign a Non-Disclosure Agreement when tasking requires access to PII.

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.

PII is not collected directly from the individual.

This system will not be the initial collection point of PII, but may be used as follow-on or archival storage. As such, the individuals have already agreed to the collection of their PII via the primary collection system.

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.

PII is not collected directly from the individual.

The Navy Active Directory and Global Address List provide PII on users. The systems uses this and other unique information to ensure the identity and manage appropriate privileges for users.

The individual isn't the source of the PII collected (except in special cases as noted above for Selected Reservists).

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.

PII is not collected directly from the individual.

Privacy Advisory

We will not obtain personally identifying information about you when you visit our site unless you choose to provide such information to us. If you choose to send email to the site webmaster or submit an on-line feedback form, any contact information that you provide will be solely used to respond to your request and not stored.

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.