



PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAVY.COM (NAVY.COM)
Department of the Navy - BUPERS

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 DITPR ID: 726 DITPR DON ID: #20346
- 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

UJI: 007-000006566

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

N01133-1

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, Departmental Regulations
5 U.S.C. 302, Delegation of Authority
4 U.S.C. 3101
4 U.S.C. 3702
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.

The Navy.com web environment is comprised of a public-facing web site housed in a commercial hosting facility. The web site is used by the general public and is the primary resource for Navy recruiting information. The purpose of Navy.com is twofold: educate interested prospects on the Navy and generate leads for recruiter follow-up.

Navy.com is a vital marketing tool. It acts as the hub for many official Navy sponsored advertising tactics which direct prospects to Navy.com for more information. Everything from television ads and radio spots to email, banner ads and social media drive traffic to Navy.com. The site attracts over 675,000 monthly visitors.

Navy.com plays a critical role in helping the Navy Recruiting Command meet its mission in several high priority professional communities. This site includes expansive sections that not only cater to General Enlisted Sailors, but also target specialty communities/ratings such as Navy Special Warfare (NSW)/Navy Special Operations (NSO), Women in Non-traditional Roles (WIN-R), Nuclear Officers, and Navy Health Care.

Prospects can interact with a wealth of information about Navy life, available career opportunities, and benefits. Users can read content, view images, and even watch videos depicting what a "day in the life" of a Navy Sailor/Officer is like.

One of the primary objectives of Navy.com is to ultimately motivate users to seek additional information on the Navy. All potential applicants are forwarded to local recruiters to continue the conversation. Navy.com generates an average of 25,000 leads per month and is the number one lead generator for the Navy Recruiting Command.

Personal information collected includes: Name, Social Security Number (SSN), citizenship, date of birth, personal cell telephone number, home telephone number, personal email address, mailing/home address, education information: high school graduate and for officers four year and higher degree information, education level completed and transcripts; Employment Information: employment history. In addition, for individuals with prior service they may also provide branch of service, military service history, reenlistment code, discharge date/type.

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

All BUPERS/Navy Recruiting Command personnel with access to the system complete the annual DoD Information Assurance Awareness training per DIACAP requirements. Navy.com is DIACAP accredited and is subject to the monthly and annual DIACAP verification/confirmation scans.

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. Because of this possibility, appropriate security and access controls listed in this PIA are to be put in place.

All systems are vulnerable to "insider threats." All System Managers will be vigilant to this threat by limiting system access to those individuals who have a defined need to access this information. There are defined criteria to identify who should have access to the applications. These individuals have gone through extensive background and employment checks.

Security perimeter protections (firewall, intrusion detection, router access control list, etc.) provided by the hosting enclave. Additionally, strict access control policies and procedures are implemented to ensure is

restricted only to those individuals with a need-to-know through role based access schema.

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.

Yes, personal information is submitted to Navy.com by the individuals as they request information about the Navy and/or request to be contacted by the Navy. They can also request that their information be removed from Navy.com should they change their mind after submitting it.

(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.

Personal information provided by the individual requesting information is completely voluntary for purposes of obtaining more information on the Navy and/or requesting to be contacted by the Navy. The individual is provided access to the site's Privacy Policy.

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.

A link to the Privacy Act Statement is provided on the register for a personal account screen, within the online application.

A link to the Navy.com privacy policy is provided on the website.

--

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.