



PRIVACY IMPACT ASSESSMENT (PIA)

For

NAVY.COM

NAVY RECRUITING COMMAND (NRC)

29 May 2009

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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 Enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

- No

d. Does the DoD information system or electronic collection have 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 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.

No

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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.

5 U.S.C. 301 and 302, Departmental Regulations

44 U.S.C. 3101, 3702

E.O. 9397

COMNAVCRUITCOMINST 1131.2D, Navy Recruiting Manual - Officer (CRUITMAN-OFF), 2 June 2009

COMNAVCRUITCOMINST 1130.8H, Navy Recruiting Manual - Enlisted, 2 April 2008

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.com is a web-based application aimed at the general public to generate viable leads for recruiting purposes. By using media and technology, the Navy, specifically, NRC HQ and field recruiters, have the opportunity to provide more in-depth information to potential recruits, the customer, thus enabling people to make an informed choice about joining the Navy.

The types of personal information collected in the Navy.com system are name, citizenship, birth date, personal and home telephone numbers, personal email address, mailing/home address, and education information.

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

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

The following controls are used to mitigate the risks:

- a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
- b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
- c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
- d) Audits. This includes review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
- e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
- f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved.

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

Navy Recruiting Command

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

Campbell-Ewald. The contracting language that safeguards PII is as follows "The contractor shall also maintain and protect PII information based on current DOD and DON rules and regulations."

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 the method by which individuals can object to the collection of PII.

Individuals are advised that collection of PII is completely voluntary. A Privacy Notice is displayed on the site informing individuals that information provided is protected from unauthorized disclosure by the Privacy Act of 1974 and that information collected may only be used to identify and process individuals interested in applying for enlistment or commissions in the United States Navy or Navy Reserve. Declining to provide information may result in not being contacted by a Navy recruiter.

(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 are advised that collection of PII is completely voluntary. A Privacy Notice is displayed on the site informing individuals that information provided is protected from unauthorized disclosure by the Privacy Act of 1974 and that information collected may only be used to identify and process individuals interested in applying for enlistment or commissions in the United States Navy or Navy Reserve. Declining to provide information may result in not being contacted by a Navy recruiter.

(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.

Required Privacy Act disclaimer is displayed throughout the site.

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.