



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Naval Facilities Acquisition Center for Training System (NFACTS)

Department of the Navy - Naval Facilities Engineering Command (NAVFAC)

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:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps: function, composition; OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS), Catalog of Navy Training Courses and Student Reporting Requirements; MCO 1580.7D Schools Inter-service Training; and E.O. 9397 (SSN), as amended.

Additional authorities:

Training Module - SECNAVINST 5300.38, DoD Instruction 5000.55, 5 U.S.C. § 301; 5 U.S.C. § 4103; 5 U.S.C. § 4115; and 5 U.S.C. § 4118.

Intern Module - NAVFAC INST 12213.1, 5 U.S.C. § 301; 5 U.S.C. § 4103; 5 U.S.C. § 4115; and 5 U.S.C. § 4118.

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.

Training Module - Required for tracking the DAWIA certification, training, and education levels of NAVFAC employees, military and civilians. This module provides a complete course management system for the Naval Facilities Institute.

Personal information collected includes name, other names used, education information, military rank, civilian grade, and office phone number.

Intern Module - Name, civilian grade, and salary of each current intern is maintained for program management. Names and civilian grades of all interns who have graduated from or left the intern program (with loss date and loss reason) are retained.

Various administrative, technical and physical security controls, such as the use of Common Access Card (CAC); use of Secure Sockets Layer (SSL), system access enabled to support user identification and authentication using DoD PKI, implementation of role-based access control within the application, and yearly security awareness training requirement are in place to mitigate the risk of PII compromise.

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

As with any other system design, there is always the risk of privacy (PII) being compromised. The privacy risks associated with PII collected is the risk of disclosure when authorized users fail to secure their workstations when not in use and a hacker breaking into the system.

These risks are mitigated through the implementation of various administrative, technical and physical security controls, such as the use of Common Access Card (CAC); use of Secure Sockets Layer (SSL), system access is enabled to support user identification and authentication using DoD PKI, implementation of role-based access control within the application, and yearly security awareness training requirement.

Risks regarding the collection, use and sharing of PII in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls.

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.

NAVFAC personnel.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

[Empty text box]

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Sunset Design (webmaster):

2.4 Security Requirements. All work under this task order shall be UNCLASSIFIED. All personnel involved in the task must have on file with the government a current background check, at a minimum a Public Trustworthiness check (SF85P). Contractor personnel touching government IT must also maintain a current OPNAV 5239/14 System Access Authorization Request. Contractor personnel must complete annual Information Assurance Awareness training in order to gain access to government IT. If the task brings the contractor in contact with any Privacy Act data or Personally Identifiable Information (PII), the contractor personnel must comply with NAVFAC Instruction 5211.1, NAVFAC Privacy Policy.

2.4.1. The contractor must comply with all applicable regulations and guidance applicable to the sensitivity of that data. Hardware firewalls, software firewalls, and Public Key Infrastructure will be used in all data transmission between the government and the non-government systems supporting the mission as mandated in COMNAVNETWARCOM ltr ser N64/579 of 15 Oct 2003.

2.4.5. If processed or stored on portable devices at the contractor's facilities, DOD Sensitive but Unclassified/Controlled Unclassified Information (SBU/CUI) data will only be stored or processed on portable devices utilizing encryption compliant with Naval Message DTG 091256Z Oct 07: DON Encryption or Sensitive Unclassified Data at Rest Guidance.

Other (e.g., commercial providers, colleges).

Specify.

[Empty text box]

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.

[Empty text box]

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

The information is not collected from the individual, it is pulled from existing systems or input by the Program Manager.

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.

The information is not collected from the individual, it is pulled from existing systems or input by the Program Manager.

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.

Training Module - Each time a student registers for a course or wants to gain access to training records, they are provided a system "Privacy Advisory" that states: "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 online feedback form, any contact information that you provide will be solely used to respond to your request and not stored". They are also provided a system "Privacy Act Statement".



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.