



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Information System for Training, Operations and Logistics (PISTOL)

Department of the Navy - 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;
E.O. 9397 (SSN), as amended;
CNICINST 5230.1, Total Workforce Management Services;
OPNAVINST 3440.17, Navy Installation Emergency Management Program.

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 Personnel Information System for Training, Operations, and Logistics (PISTOL) web based application is the Naval Construction Forces Command (NCFC) premiere tool for official unclassified intra-unit Operational and Training management for 37 globally deployed active and reserve units consisting of approximately 16,000 personnel.

The system provides a centralized capability to manage mission support resources for tactically deployed and home-ported NCFC and other expeditionary forces. PISTOL is used for hierarchical management of internal unit organizations and personnel inventory management throughout the unit to the position level (e.g. Companies, Squads, and Fire Teams, Air Detachments, Chemical, Biological, and Radiological (CBR) Teams and Water Well Teams) providing the ability to ensure units Ready For Tasking (RFT) throughout the Fleet Readiness Training Plan (FRTP). Additional NCFC resources are managed from all vantage points necessary to the expeditionary community such as Personnel Gear Issue (combat related equipment and communications gear), expeditionary training scheduling and course management, Seabee Skill Assessment, and unit movement control by name (e.g. pre-advance parties, advanced parties, and main body deployment).

PISTOL's architectural design supports a central data repository and automatic system fail-over for mission support applications, and its architectural framework enables application integration for all contingency engineering operations. PISTOL data is pushed weekly to Navy Training Management and Planning System (NTMPS) and NECC's Readiness and Cost Reporting Program (RCRP) for Unit Capabilities Assessment.

PII collected includes: Name, SSN, truncated SSN, citizenship, gender, race, date of birth, home phone, personal e-mail, home address, security clearance, spouse information, marital status, child info, military records, emergency contact, office address, business e-mail, office phone, EDIPI.

PISTOL is to be decommissioned by 30 SEP 2012.

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

The threats and ultimately the risk to identifiable data are identical to the threats and risk to sensitive or classified information as described by DoDI 8500.2. The Navy ODAA & CA have assessed the risk of PISTOL operations as acceptable.

Necessary measures have been taken to minimize the risk of unauthorized access. Access to the system is on a need-to-know basis and access is controlled by authorized personnel only. The system data availability is limited through CAC cards authentication and the use of roles and privileges assigned to individuals specific management areas.

Data encryption will be utilized when technically possible and DON approves a solution.

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.

All Naval Construction Forces Command (NCFC) Units, NAVFAC, Naval Expeditionary Combat Command (NECC), Navy Education and Training Center (NETC)

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.

The collection of PII is requested of and voluntarily provided by service members. Mission readiness is impacted if a service member fails to provide this information due to the inability to identify and satisfy training requirement gaps and to recall personnel due to emergent events.

To support NCFC mission readiness and to ensure missions are completed successfully, PII collection is necessary to provide units with the ability to track and identify personnel training gaps; to equip and train personnel; and to project out-year training requirements and potential gaps.

Many of the fields are optional and do not have to be provided, such as spouse and child information.

(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.

NCFC units will not be able to track and identify current and out-year training gaps for their personnel. Without identifying these gaps, personnel will not be assigned to receive the training required for the successful completion of their mission.

Many of the fields are optional and do not have to be provided, such as spouse and child information.

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.

The system displays the DoD Notice and Consent banner followed by the Privacy Act Statement banner. Each banner requires the user to press the Enter key to proceed.

Privacy Act Statement

Authorities:
 10 U.S.C. 5013, Secretary of the Navy;
 10 U.S.C. 5041, Headquarters, Marine Corps;
 E.O. 9397 (SSN), as amended;
 DTM-2007-015-USD(P&R) ATTACHMENT 1 2.c.8 and 2.c.11;
 COMNAVRESFORCOMINST 1500.6, 26 OCT 04;
 COMFIRSTNCDINST 3502.1, 22 OCT 09;
 DoD 8910-M, June 1998 c3.8.2.3.11.

Purposes:
 • To authenticate the identity of individuals seeking access to data for purposes of ensuring that only authorized persons may access applications and process data.
 • To permit authorized individuals to view data for purpose of verifying its accuracy and to update the data when it is not current or is inaccurate.
 • To audit user access to ensure that access is only granted to users that are authorized access to the information.

Routine Uses: System Administrators and authorized command personnel with a need to know to maintain the system and administer the program.

Disclosure: Voluntary. Failure to provide the requested information will result in a delay or termination of your request. If your request is terminated, you will not be able to access data via 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.