



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Training Management and Planning System (NTMPS)

Department of the Navy - SPAWAR - PEO EIS PMW 240

### 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  
July 2008 NAVADMIN 203/08 Combating Trafficking in Persons (CTIP) Training Policy Update  
DODI 8500.2, Information Assurance Implementation  
OPNAVINST 5351.2, Enlisted Navy Leadership Development (NAVLEAD)  
April 2009 NAVADMIN 114/09 Trafficking in Personnel Policy Update  
OPNAVINST 1500.22F, United States navy Personnel financial Management (PFM) Education, Training, and Counseling Program and 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 purpose of this system is to maintain a listing of training, education, and qualifications of Department of the Navy personnel for use by Manpower, Personnel, Training and Education (MPTE) managers.

Specifically:

NTMPS contains several applications in addition to the core data warehouse designed to meet fleet user requirements:

(1) Fleet Training management and Planning System (FLTMPS) Ashore (DADMS ID 80631) is the web-based decision support system containing detailed personnel training histories and TYCOM training requirements and status. FLTMPS features nearly a thousand standard reports and limited ad hoc capability, providing Fleet users with current status of training readiness as well as access to the latest training requirements and course related information.

(2) FLTMPS Afloat (DADMS ID 80336) is a web application that operates on afloat units running the Navy Information/Applicaton Product Suite (NIAPS) Distance Support servers version 2.3 and later. FLTMPS Afloat provides fleet users immediate access to MPT&E data in a disconnected environment.

(3) the Electronic Training Jacket (ETJ) Ashore (DADMS ID 80796) is a web application that allows Active on their individual training and education accomplishments.

(4) The ETJ Afloat (DADMS ID 81319) is a shipboard web application running on NIAPS Distance Support servers that allows Active Duty and Reserve Enlisted and Officers to view and print, from a single source, all documented information on their individual training and education accomplishments.

(5) Online Account Request System (OARS) (DADMS ID 81495) is a web application which allows NTMPS users to apply for accounts to the FLTMPS, FLTMPS Afloat and EPM applications.

(6) The Enterprise Performance Management (EPM) (DADMS ID 80485) web application is a MPT&E business Intelligence tool accessing data from the NTMPS data warehouse.

(7) Career Tools Afloat (CTA) (DADMS ID 81621) is a shipboard web application which serves as the common access point to all Sea Warrior Afloat Programs and other applications as directed.

Type of personnel information: Name, Social Security Number (SSN), Employee ID (The personnel Command PeopleSoft database generated system identification number to be used between systems passing personnel data), DoD ID number, date of birth, race/ethnicity, gender, security clearance, marital status, level of education, professional qualification and skills, training courses completed, certification received, rate/rank, status, branch of service, activity unit identification code (UIC), military records, and military awards received.

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

When PII data is collected, there is always a risk that an individual's personal data can be lost, stolen and/or compromised. The safeguards are set up in multiple layers.

Administrative Safeguards. NTMPS users will be limited to viewing data approved by their command supervisor. Screen reports will contain labels identifying the report as Privacy Act data, and For Official Use Only. Printed reports additionally will first print a page identifying the type of data and the safeguards. Access/Permission - Access to the data will be controlled through common access card (CAC). Local commands will control access to the local computers used to access the NTMPS data.

Physical Safeguards. The NTMPS servers are located in a secure area at SPAWAR-ATLANTIC NOLA Navy Enterprise Data Center (NEDC) and is in a NMCI eDMZ.

Technical Safeguards. User Access - Access to the data will be controlled through common access cards

(CAC). All data transferred will be via encrypted channels. The interface server will be protected from attempts to penetrate the firewall through the existing NEDC controls. Process Safeguards - Users will access the Operational Data Store. Process Safeguards - NTMPS users will have read only access to the data. Additionally, Host Based Security System (HBSS) is deployed on the unclassified network to provide centrally managed antivirus detection and reporting, intrusion prevention monitoring, system baseline, and removable media control. IA monitors HBSS activity from the central HBSS IA Console.

**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.

Computer Sciences Corporation

52.224 - 1 - Privacy Act Notification

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

52.224 - 2 - Privacy Act

(a) The Contractor agrees to

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies

(i) The systems of records; and (ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act;

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor

and any employee of the Contractor is considered to be an employee of the agency.  
(c) For Systems of Record,  
DD FORM 2930 NOV 2008 Page 6 of 18  
(1) Operation of a system of records, as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.  
(2) Record, as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.  
(3) System of records on individuals, as used in this clause means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

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 information is part of the member's official military record and is obtained from approved official DoD interfaces.

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

PII is not collected from the individual.

**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 from the individual.

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

- |   |  |
|---|--|
| <input type="checkbox"/> <b>Privacy Act Statement</b> | <input type="checkbox"/> <b>Privacy Advisory</b> |
| <input type="checkbox"/> <b>Other</b>                 | <input checked="" type="checkbox"/> <b>None</b>  |

Describe each applicable format.

The information is part of the member's official military record and is obtained from approved official DoD interfaces. NTMPS does not collect information directly from the individual.

**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.**