



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Learning Management System - Distance Learning (LMS-DL)

U.S. NAVY - SPAWAR

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.

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).

Sea Warrior Concept of Operations (CONOPS), (29 Nov 2007)

The Learning Management System-Distance Learning (LMS-DL) Systems Requirements Document (31 Jan 2008) formally specifies the requirements of the program Navy eLearning (NeL) shore based systems to deliver on-line, computer based training and education to Naval personnel that provides growth and development of our people in order to enhance readiness and improve capabilities in the joint war-fighting environment. NeL . . . supports new training and education methods utilizing wide information technology (IT) infrastructure of advanced tools for real-time global access to curriculum, personnel, and career data.

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 identify individuals who enroll and take computerized training courses offered through the Navy's Integrated Learning Environment (ILE). Each user will be able to create an individualized training plan, completed Web-based training courses and track their course progress. The system is located at the Naval Education Training Professional Development Technology Center (NETPDTC), Saufley Field, FL 32509-5337. Records are maintained on electronic storage media.

Types of PII collected are name, SSN, DOB, pay plan/grade, rank, occupation, UIC, military status, individualized training plan, and course progress.

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

Information could be compromised by improper handling, resulting in identity theft.

System operators participate in a comprehensive command security program. This program includes annual Information Assurance Awareness training and Privacy Act training. Operators also receive training on using appropriate data handling safeguards.

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.

The Navy's rule for accessing records, contesting contents, and appealing initial agency determinations are published in the Secretary of the Navy instruction 5211.5; 32 CFR part 701; or may be obtained from the system manager. When entering military service or civilian employment with the DON, individuals are asked to provide their SSNs which become the individual's numerical identifier and is used to establish personnel, financial, medical, and other official records (as authorized by E.O. 9397).

Individuals can object to the collection of PII by addressing written inquiries to the Program Executive Office for Enterprise Information Systems, (PEO-EIS) (ATTN: PMW 240 Program Manager), 2451 Crystal Drive, Suite 1139, Arlington, VA 22202-4804. Signed requests should contain full name, address, Social Security Number (SSN).

NOTE: Resulting consequence of refusal to permit the collection of PII will result in individuals being unable to complete required training necessary for performance of their duties.

(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.

Individuals cannot complete required training necessary for performance of their duties.

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.

DOD Notice and Consent Banner Web Page which is displayed upon entering eLearning web 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 may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.