



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Seaware Lite Learning Management System (Seaware LMS)

Department of Navy - NAVSEA - NUWC DIVNPT

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 (specifically section b.5)
E.O. 9397 (SSN) as amended

Additional Authorities:

OPNAVINST 1540.51 (NOTAL) Submarine Tactical On Board Training (STOBT)
OPNAVINST 1540.51D Submarine On Board Training (SOBT) (Specifically, section 6.b.4)
OPNAVINST 1540.52 On Board Training (OBT) Package 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.

Seaware Lite Learning Management System (Seaware LMS) is a computer based training solution designed to deliver, track, and administer training curricula onboard the US Navy submarine fleet. Seaware LMS provides an intuitive learning environment that includes powerful competency profiling features to help instructors assign, track, and evaluate student performance and progress towards completing assigned curricula. Seaware LMS provides a mechanism for reporting course completion status for inclusion in the appropriate users' service record.

Types of personal information collected includes: name, year of birth, rank, encrypted SSN

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

PII collected ranges from non-sensitive to sensitive, high risk (SSN).

These risks are mitigated by:

1. all PII is received (transmitted) over the SIPRNET; SSN is transferred in encrypted form
2. once in the database, all confidentiality controls for a MAC III Classified application, including restrictive access controls, are established
3. once no longer needed, the PII is eliminated from the database

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.

On each submarine, those concerned with training and qualifications of each crew member.

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.

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

PII is not collected directly 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 directly from the individual.

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.

PII is not collected 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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input checked="" type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Driver's License | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Birth Date | <input type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number | <input type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Military Records |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Education Information | <input type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

NOTE: Military information is Rank/Grade only; Birth date is only Year of birth; SSN is encrypted during all data transfer.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Existing DoD Information Systems:
 Fleet Training Management and Planning System (FLTMP) is a subsystem of Navy Training Management and Planning System (NTMP) covered by SORN NM01500-10.

(3) How will the information be collected? Indicate all that apply.

- | | |
|--|---|
| <input type="checkbox"/> Paper Form | <input type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input checked="" type="checkbox"/> Information Sharing - System to System | |
| <input type="checkbox"/> Other | |

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Verification and identification.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Mission-related and administrative use.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

- Yes No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- Users Developers System Administrators Contractors
 Other

Users only have access to their own information.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> Cipher Locks |
| <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks |
| <input type="checkbox"/> Key Cards | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Safes | <input checked="" type="checkbox"/> Other |

Security badges, id cards, and guards are required for all sites to gain access to submarines. Used on a classified network onboard each submarine.

(2) Technical Controls. Indicate all that apply.

- | | |
|--|---|
| <input type="checkbox"/> User Identification | <input type="checkbox"/> Biometrics |
| <input checked="" type="checkbox"/> Password | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Virtual Private Network (VPN) |
| <input checked="" type="checkbox"/> Encryption | <input type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input type="checkbox"/> External Certificate Authority (CA) Certificate | <input type="checkbox"/> Common Access Card (CAC) |
| <input type="checkbox"/> Other | |

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Access to PII
- Encryption of Backups Containing Sensitive Data
- Backups Secured Off-site
- Other

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

- Yes. Indicate the certification and accreditation status:

- | | | | |
|-------------------------------------|---|---------------|----------|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | 20110524 |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | |

- No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Members PII information is downloaded from the NTMPTS system and loaded within the Seaware LMS application.

Use, Retention, and Processing: Only personnel with the "need to know" can access a member's PII information.

Disclosure: No other personnel other than those with a "need to know" can access a member's PII information unless permission is granted from the individual in writing to release the information.

Destruction: Data is destroyed in accordance with the Navy's Records Management Manual.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

The perceived threats are primarily computer hackers, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that Seaware LMS, with its extensive collection of PII, could be compromised.

Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since Seaware LMS operates on the Sublan Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats". Sublan/Seaware LMS managers are vigilant to this threat by limiting

system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to Sublan/Seaware LMS. These individuals have gone through extensive background and employment investigations.

Mitigation:

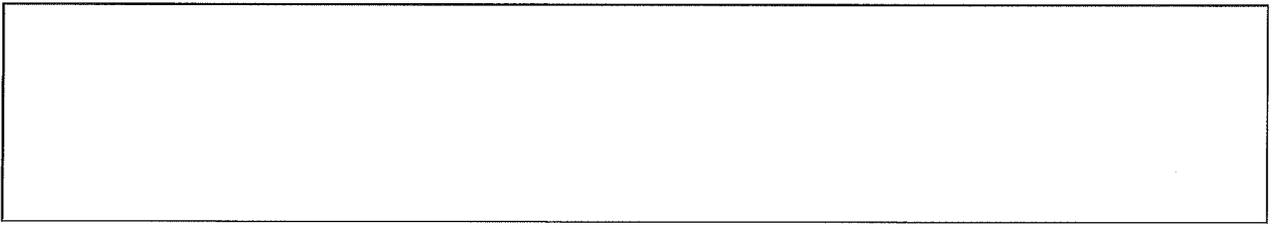
The following controls are used to mitigate the risks:

- 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: Physical security consists of placing servers that contain privileged information in a secure and protected location, to limit access to this location to individuals who would have a need to access the servers. Access to each application is limited to authorized and appropriately cleared personnel as determined by the system manager. Physical entry is restricted by use of locks and is accessible only to authorized, cleared personnel.

The Sublan servers are located in various secure locations on board each submarine.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A



SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

SADECK.JOSHUA.A.1296814837
Digitally signed by SADECK.JOSHUA.A.1296814837
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,
cn=SADECK.JOSHUA.A.1296814837
Date: 2014.06.18 12:10:57 -04'00'

Name: Joshua Sadeck
Title: Project Manager
Organization: NUWCDIVNPT
Work Telephone Number: 401-832-2113
DSN: 932-2113
Email Address: joshua.sadeck@navy.mil
Date of Review: 18 June 2014

Other Official Signature (to be used at Component discretion)

CZEPIEL.EUGENE.MICH
AEL.1011124719
Digitally signed by CZEPIEL.EUGENE.MICHAEL.1011124719
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=CONTRACTOR,
cn=CZEPIEL.EUGENE.MICHAEL.1011124719
Date: 2014.06.24 12:11:34 -04'00'

Name: Eugene M Czepiel
Title: Information Assurance Officer
Organization: NUWCDIVNPT
Work Telephone Number: 401-832-2615
DSN: 932-2615
Email Address: eugene.czepiel.ctr@navy.mil
Date of Review: 24 June 2014

**Other Official Signature
(to be used at Component
discretion)**

OBRIEN.JOHN.HARRISON
N.1228611413
Digitally signed by OBRIEN.JOHN.HARRISON.1228611413
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,
cn=OBRIEN.JOHN.HARRISON.1228611413
Date: 2014.06.30 09:32:30 -04'00'

Name: John H O'Brien
Title: Privacy Act Coordinator
Organization: NUWC DIVNPT
Work Telephone Number: 401-832-7725
DSN: 432-7725
Email Address: john.h.obrien@navy.mil
Date of Review: 30 June 2014

**Component Senior
Information Assurance
Officer Signature or
Designee**

Name:
Title:
Organization:
Work Telephone Number:
DSN:
Email Address:
Date of Review:

**Component Privacy Officer
Signature**

PATTERSON.ROBIN.W.1229
323403
Digitally signed by PATTERSON.ROBIN.W.1229323403
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=PATTERSON.ROBIN.W.1229323403
Date: 2014.09.09 18:38:36 -04'00'

Name: Robin Patterson
Title: Head, FOIA/Privacy Act Program Office (OPNAV DNS-36)
Organization: Office of the Chief of Naval Operations (CNO)
Work Telephone Number: 202-685-6545
DSN:
Email Address: robin.patterson@navy.mil
Date of Review:

**Component CIO Signature
(Reviewing Official)**

MUCK.STEVEN.ROBERT.117 Digitally signed by MUCK.STEVEN.ROBERT.1179488597
9488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597
Date: 2014.09.10 13:03:54 -04'00'

Name:	For Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	barbara.hoffman@navy.mil
Date of Review:	10 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of 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. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.