PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRIDENT Logistics Data System (LDS)
Department of the Navy - SSPO

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** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

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 DITPR ID: 315; DITPR DON ID: 14165

☐ **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 UII: 007-000001962

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 NM07421-1, NM05000-2

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:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended

Other Authorities:

OPNAVINST 4000.57G, Logistics Support of the Trident System, 19 Jan 2012

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.

TRIDENT LDS is used to plan, schedule and execute maintenance of OHIO Class SSBNs during in-port periods between strategic deterrent patrols. The system uses personal information in conjunction with collection of time and attendance data, as well as controlling user authority to access the system. Social Security Number and individual's name are used for these functions. The TRIDENT LDS architecture is undergoing enhancements that will eventually eliminate use of social security numbers in the system.

Personal information collected includes: name, full and truncated social security number, citizenship, birth date, place of birth, home telephone number, mailing/home address, security clearance, employment information.

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

Privacy risks to the individual associated with the collected PII are unauthorized access to the data or possible misuse of the data. System access controls are in place to safeguard PII and restrict access to individuals with a job related requirement to access the data. These access controls strictly limit access to the application and/or specific functional areas of the application. The controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more roles. Each role provides some combination of privileges to a subset of the database contents. Users are granted only those privileges that are necessary for their job requirements. These controls are reinforced through training of users on the authorized use and proper handling of the PII data.

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. TRIDENT LDS PII is used by the local operating site for personnel resource management functions and allocation of labor effort to specific submarine maintenance jobs. Information is also used by system administrators for the purpose of establishing and maintaining user access to TRIDENT LDS processes.

☒ **Other DoD Components.**

Specify. TRIDENT LDS PII is shared with DoD personnel and payroll management systems.

☐ **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.

All personal data contained in TRIDENT LDS is voluntarily given by the subject individual in conjunction with maintenance of the individual's information for the purpose of personnel/pay transactions, as well as maintenance of the individual's level of access to TRIDENT LDS. Failure to provide the required information would prevent the individual from being paid and work assignments managed.

(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.

Collection of individual's PII is an inherent condition of employment necessary to ensure the individual is paid and has access to LDS process required for individual's job performance.

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.	All LDS users are required to complete a System Authorization Access Request (SAAR-N) in order to obtain access to LDS applications. The SAAR-N includes a Privacy Act Statement which provides the account requester with the opportunity to concur or not with the terms of the Privacy Act notification. The account requestor determines if they want to supply PII in the appropriate blocks. However, lack of certain identifying information may impede, delay or prevent the establishment of a user account which is required for time and attendance record keeping. The account requestor's signature indicates consent with the terms. Without signature, the requester would not be able to establish an account in LDS. Systems Administrators with appropriate privileged access use the completed/signed SAAR-N to establish the requestor's user account in LDS. The LDS screens used in this process contain the following banner information: "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

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.