PRIVACY IMPACT ASSESSMENT (PIA)

For the

Standard Labor Data Collection and Distribution Application (SLDCADA)
Department of the Navy - SPAWAR (PEO-EIS/PMW 220)

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: 110 DITPT DON ID: 8937
- ☐ **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: 007-000006455

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

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 NM07421-1 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;
5 U.S.C. Chapters 53, 55, 61 and 63, Pay Rates and Systems, Pay Administration, Hours of Work and Leave;
31 U.S.C. Chapter 35, Accounting and Collection;
DoD Financial Management Regulation (DoDFMR) 7000. 14-R, Vol. 8, Chapter 5
E.O. 9397 (SSN)

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.

SLDCADA is a time and attendance system that has been chosen as the DON standard. SLDCADA allows for centralized or distributed input, provides the capability to track civilian (Federal Employees), military, as well as contractor labor hours against job order numbers for financial purposes, and hours against type hour codes for any purposes. SLDCADA can track project tasks and be used to transfer project data to a Work Breakdown Structure (WBS) for project and task tracking. Other notable features include a leave availability check, prior pay adjustments, exception reporting, ability to query DCPS files (MER and BIMER), and easy access to employee information by authorized users. Interfaces are in place with DCPS, the DOD standard financial systems (DIFMS, STARS-FL, STARS-HQ, SABRS), as well as other various local financial systems. SLDCADA is in mixed-life cycle phase. The system is bounded within the GIG by the NMCI network. Interconnections are with systems outlined above and with approximately thirty-nine local systems agreed to via up-to-date MOAs. SLDCADA is hosted by NMCI under a service level agreement at the NMCI primary Data center Pax River, MD and the NMCI Alternate Data Center China Lake, CA. System components are the SLDCADA and associated operating system software, web servers, and database servers. Daily and weekly backup is provided by NMCI under the SLA. Certified time and attendance reports are archived by using organizations and retained for six years or until a GAO audit, whichever occurs first. Data is not archived or deleted from the SLDCADA systems. This is required by law.

PII contained in SLDCADA are the federal employee's name, social security number, citizenship, and mailing/home address.

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

The privacy risk associated with the PII collected are a federal employee's identification via name, social security number and home address by unauthorized personnel or the theft of such information. Personal information is collected to associate the employee time and attendance with payroll leave and earnings in the DFAS Defense Civilian Payroll System (DCPS). Selective military and contractor personnel hours are associated via name and employee number or SSN with job order numbers for project and program performance. Only federal employee time and attendance information is forwarded to DCPS. The risks are mitigated via application security controls for self-inputer login, and access via Common Access Card (CAC), system monitoring by NMCI and SLDCADA security personnel, system security controls as outlines in the system security authorization agreement (SSAA) as certified and authorized by the Department of the Navy's NETWARCOM issued system Approval to Operate (ATO). All system users undergo annual Privacy Act training.

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. Department of the Navy local moderators and system administrators.
- Local moderators are designated by the organizations to manage account details which requires them to have access to the PII. These moderators must have IT-2 or greater sensitivity level background investigations and are designated by their supervisor to have a valid need-to-know for PII in order to complete their job.
- SLDCADA System Administrators have extensive access to the system, which includes PII. They must have IT-1 sensitivity level background investigation and designated by their supervisor to have a need to know for PII in order to complete their job. These can be government or contractors

but not Foreign Nationals. Their system functions must be accessed via CAC and PKI authentication.

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service

☒ **Other Federal Agencies.**

Specify. Executive Office of the President

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Contractor varies depending on customer location. This is at the discretion of our customer sights and their PCO's and COR's; controlled and changed at their discretion. The language of the contract and their protection of the PII is the responsibility of the individual organization commands and their Contracting team. Confirmed that the two Privacy FAR clauses are mandatory in all contracts: (a) The clause at 52.224-1, Privacy Act Notification. (b) The clause at 52.224-2, Privacy Act.

☐ **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.

Federal employees can not object because this information is fed to the payroll system by DCPS (i.e.., the PII is not collected from the individual). Without the PII the individual could not be paid.

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.

By working for the federal government a federal employee must provide the required PII to be employed and paid. Military members are generally in the system if they certify federal employee time and attendance and or have their respective labor hours tracked against job order numbers for Work Breakdown Structure (WBS) purposes.

Selected contractors' labor hours are also tracked for WBS purposes. The government activity requesting contractor data included in SLDCADA would need to negotiate with the contracting agency to include them in the system. It is the responsibility of the contracting agency to ensure that contractor personnel understand that providing data covered under the privacy act will be required to access the SLDCADA system. SLDCADA system provides a message on each window within the application stating that this window may contain data subject to the Privacy Act. Contractor data does not get sent to other systems.

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.

Federal employee PII in SLDCADA is obtained from the DFAS Defense Civilian Pay System (DCPS) with each Master Employee Record (MER) not 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.