PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Standard Integrated Personnel System (NSIPS)
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**	☐	**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: 108 DITPR-DON ID: 15705
☐	**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 007-000001371

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 N07220-1

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 authorities:

10 U.S.C. 5013, Secretary of the Navy
E.O. 9397 (SSN), as amended.

Specifically, per 10 U.S.C. 5013, the Secretary of the Navy is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Navy, including; Organizing, Mobilizing, Demobilizing, Servicing, and Administering (including the morale and welfare of personnel). NSIPS is the Navy's field level tool for gathering personnel data, and is the fundamental tool to gather the information required to meet the responsibilities laid out in 10 U.S.C. 5013.

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 provide secure worldwide personnel and pay support for Navy members and their commands. To allow authorized Navy personnel and pay specialists to collect, process, modify, transmit, and store unclassified personnel and pay data. To support management of leave and pay entitlements and deductions so that this information can be provided to the Defense Finance and Accounting Service (DFAS) for payroll processing and preparation of the Leave and Earnings Statements (LES).

Personal information collected includes: Name, Social Security Number (SSN), Truncated SSN, DoD ID Number, Citizenship, Legal Status, Gender, Birth Date, Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Personal Email Address, Mailing/Home Address, Religious Preference, Security Clearance, Mother's Maiden name, Mother's Middle Name, Spouse Information, Marital Status, Child Information, Financial Information, Employment Information, Military Records, Emergency Contact Information, Education Information.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of mature (e.g. fire, flood, etc.). All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that NSIPS, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access control listed in this PIA are in place. Since NSIPS operates on the NMCI Network and ship networks, 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." NSIPS 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 NSIPS. These individuals have gone through extensive background and employment investigations.

NSIPS is an accredited system operating within the Navy Marine Corps Intranet enclave. It operates within a Defense in Depth Architecture strategy IAW Navy and DoD security policies. Access to the system requires a valid CAC or PKI certificate, as well as, user id, and password. Access to the physical server environment is controlled via two cipher locked doors. Personnel who are granted access to operate the system must be US citizens and cleared at the secret level.

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. .

Bureau of Naval Personnel
Naval Education and Training Command
Naval Installations Command
Navy Medicine Information Systems Support Activity
Navy Reserve Force
Space and Naval Warfare Systems Command

☒ **Other DoD Components.**

Specify. Air Mobility Command

Defense Finance and Accounting Service
Office of the Secretary of Defense

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

As stated Section 6.3 Data Protection in the SRA International, INC Performance Work Statement for the Indefinite Delivery/Indefinite Quantity (ID/IQ) Contract N00039-14-D-0001...
"The Contractor shall comply with the DON Privacy program per SECNAVINST 5211.5E.

The Contractor shall ensure all categories of sensitive information, including PII, are secured and in compliance with all IA Controls from the DoDI 8500.2, specifically IA Controls DCFA-1 and DCSR-2. Compliance includes the encryption of "data in transit" and "data at rest" as required by the data owner.

The Contractor shall comply with DON CIO MSG DTG 171952Z APR 07 to ensure that all Personally Identifiable Information (PII) is properly safeguarded. The requirement under the E-Government Act of 2002, mandates that all PII be protected. In addition, systems processing PII must have completed a Privacy Impact Assessment (PIA) and register that PIA with DON CIO.

The Contractor shall provide controlled access to prevent unauthorized access to DoD systems and information using identification and authentication as well as encryption."

☐ **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.

PII is not collected directly from the individual. See Section 3, question a. (2).

(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.

PII is not collected directly from the individual. See Section 3, question a. (2).

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. See Section 3, question a. (2).

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.