PRIVACY IMPACT ASSESSMENT (PIA)

For the

My Navy Portal (MNP)
Department of the Navy - SPAWAR - 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: 16665 DITPR-DON: 22608
☐	**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: 007-000005872

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 DMDC 02 DOD; DMDC 12 DOD; N07220-1;N06110-1,

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 | Not required. Does not collect PII directly from the individual. Pulls PII from other authorized systems. Confirmed with OPNAV DNS-15.

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 DMDC 02 DOD authorities:

55 U.S.C. App. 3, Inspector General Act of 1978
5 U.S.C. Chapter 90, Federal Long-Term Care Insurance
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness
10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits
10 U.S.C. Chapter 54, Commissary and Exchange Benefits
10 U.S.C. Chapter 55 Medical and Dental Care
10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated
10 U.S.C. Chapter 75, Deceased Personnel
10 U.S.C. 2358, Research and Development Projects
20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act
31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management
42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148)
42 U.S.C. 1973ff, Federal Responsibilities
50 U.S.C. Chapter 23, Internal Security
DoD Directive 1000.04, Federal Voting Assistance Program (FVAP)
DoD Instruction 1100.13, Surveys of DoD Personnel
DoD Instruction 1341.2, DEERS Procedures

DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters
Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
38 CFR part 9.20, Traumatic injury protection
38 U.S.C. Chapter 19, Subchapter III, Service members' Group Life Insurance
42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); and E.O. 9397 (SSN), as amended.

SORN DMDC 12 DOD authorities:

5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes
10 U.S.C. 137, Under Secretary of Defense for Intelligence
DoD Directive 1145.02E, United States Military Entrance Processing Command (USMEPCOM)
DoD 5200.2R, DoD Personnel Security Program (PSP)
DoD 5105.21, Sensitive Compartment Information Administrative Security Manual
DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction
DoDI 5200.02, DoD Personnel Security Program (PSP)
DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program
DoDI 5220.22, National Industrial Security Program (NISP)
Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors
E.O. 9397 (SSN), as amended.

SORN N07220-1 authorities:

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

SORN N06110-1 authorities:

10 U.S.C. 5013, Secretary of the Navy
OPNAVINST 6110.1 Series, Physical Readiness Program
DoD 6025.18-R, DoD Health Information Privacy Regulation
E.O. 9397 (SSN), as amended.

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 My Navy Portal (MNP) is to enable the Navy user to accomplish Manpower, Personnel, Training and Education (MPT&E)-related tasks through a common Graphical User Interface (GUI) that greatly enhances the user's experience and provides a single point of entry as well as a single sign-on (SSO) capability. MNP will implement a production-integrated, Common Access Card (CAC)-protected portal that will be driven by a single Authoritative Data Environment (ADE) to access, validate, and perform various data-driven tasks. MNP provides a common GUI across all current content, collaboration, capability, and customer service resources. MNP brings together relevant data into a single consolidated logical workspace that leverages a common menu system and page templates to harmonize the look and feel, providing a quality user experience through integration, prototyping, and related engineering efforts and technical framework. Employing a central knowledge management framework, the MNP portal define user MPT&E-related tasks and permit users to track the process tasks transparent to the hosting of the data, by producing a congruent intuitive GUI-based capability. In summary, MNP will enable the Navy user to securely review authoritative data to enhance the pursuit of their goals and achievements through a technically advanced web-based user experience.

Because MNP will directly interface with the ADE, and because the strategic vision is for MNP to be the one-stop-shop for Sailor's to view information about themselves, MNP has the potential to access all types of

information that is typically held in a Sailor's personnel record (i.e. promotion, training, readiness, and dependent data).

PII collected: See section 3, question a. for complete listing. The SSN is not collected.

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

Risks:

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, 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 MNP, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA will be put in place.

Since MNP operates on a Navy owned 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. This risk is mitigated by using an automated script to both disable and enable security features.

All systems are vulnerable to "insider threats." MNP managers will be 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 MNP. These individuals have gone through extensive background and employment investigations.

Mitigations:

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. Access to data is provided on a need-to-know basis and is encrypted in transit.

c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner. Data is provided by an authoritative source and is encrypted in transit. Changes in the data are typically not made in MNP since it acts primarily as a mechanism for Sailors to view data only.

d) Audits. This includes review and examination or 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. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers.

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. Local Command Personnel (Commanding Officer, Executive Officer, Career Counselor) , Navy Personnel Command, BUPERS.

☐ **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. All PMW 240 contracts contain the following language:

The Contractor shall comply with the DON Privacy program per SECNAVINST 5211.5E.

The Contractor shall ensure all categories of sensitive information, including Personally Identifiable Information (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 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 MNP contract contains the required FAR privacy clauses.

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.

(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.

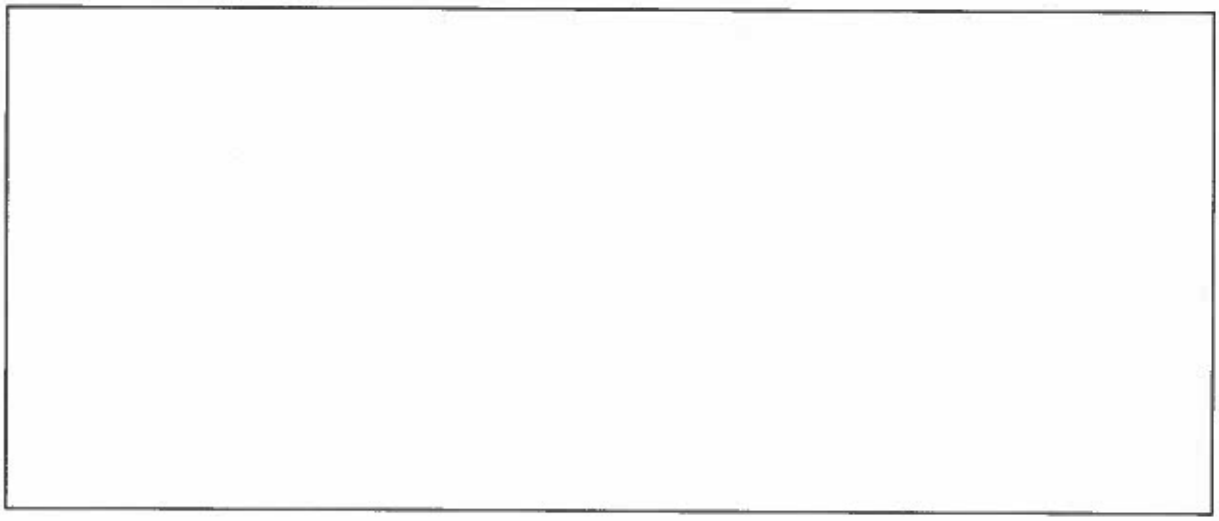
k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **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.