PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

My Navy Portal (MNP)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

11/13/18

SPAWAR - PMW 240

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The purpose of the My Navy Portal (MNP) , herein called MNP, is to enable the Navy affiliated 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. Collection of data supports official Navy MPT&E and system management functions.

Because MNP will directly interface with the Authoritative Data Environment (ADE), and because the Full Operational Capability for MNP to be the one-stop-shop for Sailors to view information about themselves, MNP will access all types of information that is typically held in a sailors personnel record.

MNP implements a secure Public Key Infrastructure (PKI) protected portal utilizing Common Access Card (CAC) and CAC-derived National Institute of Standards and Technology (NIST) standards compliant security controls. The system will be driven by an 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.

The system will be integrated in to the Authoritative Data Environment (ADE) system and SORN

PII collected: Full Name, Department of Defense IDentifier (DOD ID) number, citizenship, home/cell phone, mailing/home address, official duty address, work email address, marital status, official duty telephone , persona email address, position/title, rank/grade, gender, legal status, Employment Information - employment history; Military Records - Personnel service jackets and service records. To include correspondence and records concerning classification, assignment, distribution, promotion, advancement, performance, recruiting, retention, reenlistment, separation, readiness, training, education, morale, personal affairs, dependent data, benefits, entitlements, discipline and administration of naval personnel.; Education Information - highest level of education, courses taken, and courses completed.; Security Information - Security clearance; Child Information - Number of dependents, name, and age.; Emergency Contact Information - Name, phone, and email.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Mission related use. PII is collected to support Sailors, their families, and their command in execution of MPT&E-related tasks. PII is also collected to support communication with the Sailor and their dependents as relates to service requests about the MNP system and partner systems.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Sailors cannot object to PII collection about themselves because data collected is requird to manage their Navy career. Sailors can object to PII collected on their dependents by not participating but then the Sailor and the dependents would not be provided benefits for which they might otherwise be eligible.

f. 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.

Providing information is considered consent. All purposes of the data collected is for official Navy functions that support Sailor career management are required for MPT&E-related tasks. Where unofficial uses may be allowed, MNP provides the option to not participate in those functions with the penalty of not receiving service or benefits related to that task.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

Privacy Notice
1. This My Navy Portal (MNP) public site is an official U.S. Navy World Wide Web site that is provided as a public service by PEO-EIS PMW 240.
2. Any communications using, or data stored on, this United States Government (USG) Information System (IS) are not private; are subject to routine monitoring, interception, and search; and may be disclosed or used for any USG authorized purpose.
3. Information presented on this service not identified as protected by copyright is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.
4. For site management, information is collected for statistical purposes. This USG computer system uses software programs to create summary statistics that are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
5. For site security purposes and to ensure that this service remains available to all users, this USG IS routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network defense, quality control, identifying unauthorized attempts to upload or change information, employee misconduct, law enforcement, and counterintelligence investigations.
6. Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and from time to time, from which top-level domain users are access the site. This data is scheduled for periodic destruction in accordance with National Archives and Records Administration guidelines.
7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.
8. Personally Identifiable Information (PII) is any information about an individual that can be used to distinguish or trace an individual 's identity and that is linked or linkable to specified individual, alone or when combined with other personal or identifying information. (DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014) We do not obtain PII about you when you visit our site unless you choose to provide such information to us. We will obtain PII about you when you login to the site in order to help you conduct career management. If you choose to send email to the site webmaster or submit an online feedback form, any contact information that you provide will be solely used to respond to your request and not stored.
9. MNP will receive your personal information from, and send your personal information to, other Navy and Department of Defense (DoD) systems in response to your actions on the MNP system. Examples include when you submit a request, when you view your record, ask for help, apply for special programs, request changes or corrections to your personnel record(s), and perform other career and human-resource management functions.

If you have any questions or comments about the information presented here, please forward them to MNP_Helpdesk@navy.mil.

PRIVACY CONCERNS

If you have a privacy question, or you know or suspect a privacy disclosure on this website, contact the help desk at MNP_Helpdesk@navy.mil and ask for your request to be directed to the PMW 240 Privacy Officer.

COOKIE DISCLAIMER

Per Office of Management and Budget (OMB) directive M-10-22 ("Guidelines for Online Use of Web Measurement and Customization

Technologies") dated 25 June 2010, this site is allowed to use web measurement technologies to remember a user's online transactions in order to conduct measurement and analysis of usage or to customize a user's experience. This technology incorporates the use of Tier 2 multi-session cookies where no PII is collected. We will not use this technology to track user individual-level activity on the Internet outside of the MNP system, nor to share data with entities outside the Navy or DoD.

CLIENT SIDE OPT-OUT

Site visitors can opt out of web measurement and customization technologies by changing the settings of their web browser. Please refer to http://www.usa.gov/optout_instructions.shtml for general instructions on how to opt out.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Within the Navy MPT&E community of the DON, with individual commands where the Sailor or dependents may be assigned, and activities the Sailor or dependents may be utilizing for specific services.
☒ Other DoD Components	Specify.	With DOD agencies that provide status or services related to MNP users including DMDC, DEERS, DFAS.
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Access is provided to a limited number of personnel from a set of contractors as necessary to provide service to Sailors, or to manage the systems upon which the information resides. Contractors include: Katmai Services Inc. IBR Corporation Millennium Corporation Other contractors supporting partner systems with MNP that are also contracted by Navy to support MPTE functions. Each contractor has appropriate FAR language in their contracts. All PMW 240 contracts 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 Identifieable Information (PII) are secured andin 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 a completed Privacy Impact Assessment (PIA) and register that PIA with DON CIO. The MNP contract contains the required FAR privacy clauses listed. 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. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [x] Individuals
- [x] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [x] Databases
- [ ] Commercial Systems

Authoritative Data Environment (ADE), Defense Manpower Data Center (DMDC), Defense Enrollment Eligibility Reporting System (DEERS), Defense Finance and Accounting System (DFAS)

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [x] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [x] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [x] Telephone Interview
- [x] Website/E-Form

MNP will support Sailors with multiple existing forms from other organizations by providing templates to fill-in and submit those forms in web-based format. Any exisiting form used will be displayed with its form number.

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier NM01500-10

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N/A

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

System does not contain records. Because MNP will directly interface with the Authoritative Data Environment (ADE). So ADE owns the DATA or records.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN NM01500-10, Navy Training Management and Planning System (NTMPS) (June 28, 2012, 77 FR 38608), authorities: 10 U.S.C 5013, Secretary of the Navy; July 2008 NAVADMIN 203/08 Combating Trafficking in Persons (CTIP) Training Policy Update; DODI 8500.2, Information Assurance Implementation; OPNAVINST 5351.2, Enlisted Navy Leadership Development (NAVLEAD); April 2009 NAVADMIN 114/09 Trafficking in Personnel Policy Update; OPNAVINST 1500.22F, United States Navy Personnel Financial Management (PFM) Education, Training, and Counseling Program; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

MNP Cloud does not require an OMB number at this time per the guidelines in DoD Manual 8910.01. NMP Cloud does not collect information directly from any member of the public. DOD ID is extracted from the CAC for verification.