PRIVACY IMPACT ASSESSMENT (PIA)

For the

Health Promotion and Wellness Dashboard (HPWD)
Department of the Navy - Bureau of Medicine and Surgery (BUMED)

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	eMASS ID: 6853
☐	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

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

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.

BUMEDINST 6110.13A states that BUMED, through the Surgeon General, is the Chief of Naval Operation's (CNO) principal advisor on health service programs within the DON, and is the subject matter expert on the DON's Health Promotion Program.

Navy Medical Departments will serve as a community-based resource in support of health promotion programs. This application will be used to collect data to provide measures of effectiveness that will be in accordance with provider enterprise/strategic plan/whole goals and will use continuous process improvement tools (e.g., Lean Six Sigma) and administer health promotion and wellness awards/recognition programs.

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.

HPWD is a web based tool used to promote health and wellness among service members and DoD personnel. The dashboard consists of three primary products. The first of these is the Blue H product. This is used to assess the eligibility for the Surgeon General's Blue H award for Navy and Marine Corps facilities. The second product is m-Neat. This system is a portal that allows Naval and Marine Corps facilities to evaluate the health level of the products being offered for consumption at a particular location. The third product is the Crews into Shape product. This is used once a year to track a team's progress in the DoD's annual fitness and healthy eating promotion event.

Types of personally identifiable information (PII) collected by the system includes: name, personal email address, employment information (office email address, work phone number), military records (rank, location/ facility information), personal email address and phone number.

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

Where as all systems are at risk and vulnerable to unauthorized access or intrusions such as hacking, the HPWD data is processed on an accredited network in the Navy Medicine domain in accordance to DoD requirements and authorized by the Navy Operational Designated Approving Authority (ODAA)."

The risk that HPWD data could be compromised have been evaluated and determined to acceptable because the system has been properly secured with the appropriate administrative, technical, and physical safeguards listed in the PIA.

The HPWD user risk concern is considered acceptable because all users are required to initially complete and annually re-take DoD approved training for Cyber Awareness, Privacy Act and HIPAA that addresses privacy issues, system uses and information management.

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. Personnel supporting Navy and Marine Corps public health promotion and wellness responsibilities

☐ **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.

☐ **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.

The participants can elect to not participate in the programs.

(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.

The participants can elect to not participate in the programs.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

The following DoD Notice and Consent is displayed when a user logs into HPWD:

DEPARTMENT OF DEFENSE NOTICE AND CONSENT
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. This site may contain a highest level of sensitive or un-classified information. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

A following Privacy and Security Notice is also displayed:

PRIVACY AND SECURITY NOTICE
1. {Application Name} is provided as a public service by the Navy and Marine Corps Public Health Center.
2. 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.
3. For site management, information is collected for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which 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.
4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DoD websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines.
6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department websites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or

agencies. The Department of Defense does not keep a database of information obtained from the use of WMCT. General instructions for how you may opt out of some of the most commonly used WMCT is available at http://www.usa.gov/optout_instructions.shtml.
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 (18 U.S.C. § 1030).
8. If you have any questions or comments about the information presented here, please forward them to {point of contact email address}.

Information Collected from this website for Statistical Purposes

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.