PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Readiness Reporting System (MRRS)
Department of the Navy - SPAWAR (SPAWAR Systems Center (SSC) Atlantic)

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: 723 DITPR DON ID: 20087
☐	**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 007-000001646

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 NM06150-6

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
10 U.S.C. 5041, Headquarters, Marine Corps
BUMED Note 6110, Tracking and Reporting Individual Medical Readiness Data
SECNAVINST 6120.3, Secretary of the Navy Periodic Health Assessment for Individual Medical Readiness
Pub. L. 108-735, Section 731 Ronald Reagan National Defense Authorization Act,
10 U.S.C. 136(d), Under Secretary of Defense for Personnel
10 U.S.C. 671, Members not to be assigned outside United States before completing training
DoD 6025.18-R, DoD Health Information Privacy Regulation
E.O. 9397 (SSN), as amended.

Other authorities:

BUMED Note 6110.14 CH-1 Dated 16 JUN 2009, Tracking and Reporting Individual Medical Readiness Data (references MRRS as a collection point for this data)

SECNAVINST 6120.3 CH-1 Dated 01 DEC 2009 - Secretary of the Navy Periodic Health Assessment for Individual Medical Readiness (lists MRRS as a system to collect this data).

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 MRRS system mission is to assist all Navy, Marine and Coast Guard with assessing the medical readiness state of each member, unit, activity, or command. Their clinics use MRRS as a data-entry station to update the medical status of their members when any readiness medical status changes. MRRS tracks information related to physical exams, dental status, illnesses/injuries, pregnancies, and immunizations. An extensive reporting facility is implemented to provide rapid up-to-date information to the decision-makers. The MRRS system also provides capabilities for managing the process for claims resulting from on-the-job illnesses or injuries. MRRS complies with a Secretary of Defense directive to provide current anthrax and small pox immunization status.

PII information collected by MRRS includes the members name, SSN, gender, date of birth, place of birth, home telephone number, home address, and medical information (dates of immunizations, dates of medical test, dates of physicals).

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

Potential threats/risk that may impact the integrity, availability and confidentiality of the MRRS system include hardware/software failure, and fire wall issues.

All systems are at risk because may be vulnerable to unauthorized intrusion and hacking. There are risk that MRRS with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

Since MRRS operates on the NMCI 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.

All systems are vulnerable to "insider threats". MRRS 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 MRRS. These individuals have gone through extensive background and employment investigations.

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. Navy Medical personnel entering and retrieving records, and commanders verifying their units medical readiness

☒ **Other DoD Components.**

Specify. Marine commanders verifying their units medical readiness

☒ **Other Federal Agencies.**

Specify. Coast Guard Medical personnel entering and retrieving records, and commanders verifying their units medical readiness

☐ **State and Local Agencies.**

Specify.

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

Specify. eVenture Technologies, 52.224 - 1 - Privacy Act Notification and 52.224 - 2 - Privacy Act are incorporated by reference in Section I of the contract.

☐ **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.

The data is obtained from interfaces or from the member. The data provided by the member is needed to determine medical readiness. When data is collected during the recruiting phase each applicant is advised of their rights under the Privacy Act of 1974.

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.

The data is obtained from interfaces or from the member. The data provided by the member is needed to determine medical readiness.

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.	Privacy Act Statement is displayed on all reports which contain PII information Privacy Advisory is displayed and must be acknowledged prior to logging on to the application.

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.