PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Medicine Online (NMO)
Defense Health Agency (DHA)

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	196
☐	**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: 007-000000492

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 N06150-2

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.

10 U.S.C. 55 Medical and Dental Care;
10 U.S.C. 1095, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act
10 U.S.C. 5132, Bureaus: distribution of business; orders; records; expenses
44 U.S.C. 3101, Records management by agency heads; general duties
5 CFR 339.101-306, Coverage;
42 CFR 290DD Substance abuse among government and other employees;
DoDD 6485.1 Human Immunodeficiency Virus-1 (HIV-1);
Dod 6025.18-R "DoD Health Information Privacy Regulation"

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 Navy Medicine Online (NMO) serves a vital role in the overall process of collecting, analyzing, and brokering medical readiness data to and from critical and authoritative Department of Defense (DoD) data sources into one common operational view that can be drilled down into individual units and personnel as needed. Data is only provided to DoD entities.

NMO provides for management of Navy medical/dental data in a data warehouse to support Navy operational commanders and Navy Medicine/Dental personnel in managing and reporting individual medical/ dental readiness. NMO does not actively collect PII as a source system. It provides reliable data through web-based, data brokering, database operations and networked services.

NMO provides case management tools that provide an automated means to input and track waiver requests through their approval or disapproval. The tools are used to support:

-medical waiver requests for USN/USMC officer accessions programs
-medical waiver requests for USMC enlistments
-medical waiver requests for basic training medical issues for USN/USMC,
-track medical issues that may impact US Naval Academy midshipmen service selection process and commissioning, incapacitation of dependent waiver requests
-special duty medical waivers requests for submarines, spec ops, etc.

PII collected about individuals include: name, other names used, SSN which is being replaced by the DoD Electronic Data Interchange Personal Identifier (EDIPI)/other ID number, citizenship, gender, race/ethnicity, birth date, place of birth, personal cell phone number, home phone number, personal e-mail address, mailing/home address, religious preference, mother's maiden name, mother's middle name, spouse information, marital status, child information, medical information, disability information, law enforcement information, employment information, military records, emergency contact, and education information.

The sources of the data identified above are existing DoD information systems to include: Shipboard Navy Automated Processing (SNAP) Automated Medical System (SAMS), Theater Medical Information Program-Maritime (TMIP-M), Individual Medical Readiness (IMR) Lite, Dental Common Access System (DENCAS), Immunization Data Processing, Navy Immunization Tracking System (ITS), Limited Duty Sailor Marine Readiness Tracker (LIMDU SMART), Expeditionary Medicine Platform Augmentation, Readiness and Training System (EMPARTS), Medical Readiness Reporting System (MRRS), MHS Genesis, Integrated Case Management (ICM) Tool (Medical Waiver Program (WebWave), Incapacitation of Dependents (INCAP) application, Special Duty Medical Waiver Process, Midshipmen Medical Information System (MEDMIDS), Navy Standard Integrated Personnel System (NSIPS), and Defense Enrollment Eligibility Reporting System (DEERS).

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

All systems are vulnerable to "insider threats." NMO managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. Personnel who have access to NMO are medical personnel or personnel who enter medical waiver cases. There are defined criteria to identify who should have access to NMO. 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.

☒ **Other DoD Components.**

Specify. NMO manages medical readiness data to and from critical and authoritative data sources into one common operational view. NMO also provides case management for medical waivers and supports processing of approval/ disapproval letters for medical waiver cases.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. The vendor is CACI. The Vendor follows Privacy and HIPAA regulations in accordance with DoD 6025.18-R “Department of Defense Health Information Privacy Regulation,” January 24, 2003. SSC Atlantic meets the definition of Business Associate. Therefore, a Business Associate Agreement is required to comply with both the HIPAA Privacy and Security regulations. This clause serves as that agreement whereby SSC Atlantic agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and in DoD 6025.18-R.

☐ **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.

NMO receives PII from a system-to-system interface. NMO does not collect PII directly from individuals.

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.

NMO receives PII from a system-to-system interface. NMO does not collect PII directly from individuals.

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.