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:

Navy Medicine Enterprise Web Services (NME WS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

03/17/2026

Navy Bureau of Medicine and Surgery (BUMED)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

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

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ 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 Navy Medicine Enterprise Web Services (NME WS), is managed by Navy Bureau of Medicine and Surgery (BUMED) personnel and the Defense Health Agency (DHA) DCOPS-DSOCC team. The NME WS is a cloud platform acquired through the DHA Cloud Broker Services (CBS) leveraging Amazon Web Services (AWS) infrastructure and services, providing interconnectivity and information centralization across all Navy Medicine Enterprise echelons. The environment is designed for scalability, resilience, and high availability, utilizing a multi-Availability Zone (AZ) architecture and robust security controls to protect sensitive Protected Health Information (PHI) and Personally Identifiable Information (PII). PHI/PII of military members of the armed forces and DoW Civilians may be disseminated/ transferred in some systems, applications, and security controlled through limited access, based on role-based permissions. NME WS will be the cloud platform for numerous applications, data visualizations, warehouses, repositories, and any other digital requirement from the Navy Surgeon General. This environment will promote knowledge sharing and unification, deterring siloing and duplicative data efforts, and strengthen Navy Medicine Enterprise leadership's ability to make time critical decisions more efficient and decisively.

NME WS serves as a platform for numerous data-driven applications, including (but not limited to) Data Analytics, Govconnect/AI, Independent Duty Corpsman Reporting System (IDCRS), Emergency Medical System (EMS) application, SEMOSS and on demand as required by the system owner, the Navy Bureau of Medicine (BUMED) Program Management Office (PMO). In the event an application introduces additional data that creates new privacy risks introduced to NME WS environment that this PIA does not accurately describe therein, this PIA will be amended to reflect as such. The underlying data utilized by NME WS primarily consists of the CIC Data Warehouse that encompasses Military Health System (MHS) data sources outlined in Section I of this PIA whose purpose is to collect Personally Identifiable Information (PII) and Protected Health Information (PHI). Personally Identifiable Information (PII) may include numerous types of PII including employee and beneficiary contact information, military information, demographic information, and Protected Health Information (PHI).The PII/PHI collected, maintained, analyzed and transmitted is used by government analytics personnel, program managers, system managers and other workforce members with a need to know. Data sourced from CIC may be shared within BUMED enterprise, Defense Health Agency, Chief of Naval Operations and Marine Corps.

Access to this information is controlled by the Chief Data and Artificial Intelligence Officer. The system of records is supported by contractors who have appropriate clearance, federal acquisition regulation privacy, and cybersecurity requirements stipulated in their contracts. A Nondisclosure Agreement is signed before being given access to N58 (formerly known as CIC) Assessments and Analytics. Workforce members who have access to the data are required to complete mandatory and supplemental privacy and cybersecurity training in accordance with Defense Health Agency (DHA), Department of the Navy (DON), and Department of Defense (DoD) policies.

NME WS is owned and managed by the BUMED Program Management Office (PMO).

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)*

The PII is collected for a variety of uses, both mission-related and administrative. Primarily, the PII is required for workforce and patient identification, verification, and authentication for readiness tracking purposes, computer matching, and data analytics. Additionally, the PII could be used for data matching when interfacing and sharing data with external manpower, personnel and healthcare systems. Mission and Administrative related uses of the PII include personnel availability, unit readiness, and statistical analysis of health and fitness metrics. PII is not used for testing or research purposes.

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.

Individuals do not have the opportunity to object to the collection of their PII /PHI because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the collection.

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.

Individuals do not have the opportunity to object to the collection of their PII /PHI because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the collection.

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

This system is not the initial collection point for the PII. The PII is obtained from an existing DoD information system or electronic collection, therefore no Privacy Act Statement or Privacy Advisory is required.

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

☒ Within the DoD Component	Specify.	Navy Bureau of Medicine and Surgery (BUMED)
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Defense Health Agency (DHA), Department of Navy (OPNAV & Marine Corps)
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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.)*		Contractors supporting N58 initiatives: Teledyne Brown, Center for Naval Analyses, Deloitte, Johns Hopkins University Applied Physics Lab, Booz Allen Hamilton, Accenture, Palantir, Altarum, KPMG The following language is contained in the above contracts in accordance with Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, and DoDM 6025.18, "Implementing HIPAA Privacy Rule in DoD Health Care Organizations," March 13, 2019.
	Specify.	Personally Identifiable Information (PII) and Protected Health Information (PHI). The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with

Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management.

☐ 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)*

☐ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☐ Databases
☐ Commercial Systems

Military Health System (MHS) data sources:
Medical Data Repository (MDR)
MHS Mart (M2)
MHS GENESIS
Defense Medical Human Resources System internet (DMHRSi)
Joint Medical Asset Repository (JMAR)
Relias Education and Training Platform
WebWave
Centralized Credentials Assurance System (CCQAS)
Humana/ Tricare East and West
Financial Management Information System (FMIS)

Navy Systems:
Expeditionary Medicine Platform Augmentation Readiness Training System (EMPARTS)
Limited Duty Sailor and Marine Readiness Tracker System (LIMDU SMART)
DON Bureau of Personnel (BUPERS) Systems (FLTMPS)
Navy Manpower Planning and Budget Systems (NMPBS)
Corporate enterprise Training Activity Resource System (CeTARS)
Navy Standard Integrated Personnel System (NSIPS)
Medical Readiness Reporting System (MRRS)

DoD Systems:
Defense Manpower Data Center (DMDC)
Defense Medical Logistics Standard Support (DMLSS)

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

☐ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☒ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☐ Telephone Interview
☐ Website/E-Form

Transfer of files via DoD Safe Data System Download and Data Sharing.

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.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

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. GRS 6.5, item 010 (DAA-GRS-2017-0004-0001)

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

(3) Retention Instructions.

FILE NUMBER: 201-22
DISPOSITION: Temporary. Destroy when 3 years old, or when no longer needed for business use, whichever is later.

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.

Authorities include: 5 U.S.C §301 "Departmental Regulations"; 10 U.S.C §142 "Chief Information Officer"; 40 U.S.C §11315 "Agency Chief Information Officer"; 44 U.S.C §3506 "Federal Agency Responsibilities"; and 44 U.S.C §3554 "Federal Agency Responsibilities." Additional authorities to collect information are specific to the information systems or electronic collections of NME WS users and addressed in the privacy impact assessment for those respective information systems and electronic collections.

Public Law 113-101, Digital Accountability and Transparency Act of 2006, as amended in 2014; Public Law 113-291, Federal Information Technology Acquisition Reform, 2015; 10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 117, Readiness Reporting System; 10 U.S.C. 482, Readiness Reports; 31 U.S.C. 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Directive 7730.65, Department of Defense Readiness Reporting System; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; DoDM 6025.18, Implementing HIPAA Privacy Rule in DoD Health Care Organizations and E.O. 9397.

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.

The information collected in this system and is not considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3, paragraph 8b(5).