

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:

Expeditionary Medicine Platform Augmentation Readiness Training System (EMPARTS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

05/25/23

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 | <input checked="" type="checkbox"/> | 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 |
| <input checked="" type="checkbox"/> 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.

Expeditionary Medicine Platform Augmentation Readiness Training System (EMPARTS) is used by Plans, Operations, and Medical Intelligence Officers (POMI) and Manpower Staff to manage and track readiness of personnel and assignments to deployable platforms [e. g. Expeditionary Medical Facilities (EMFs), United States Marine Corps (USMC) Health Services Support (HSS), and Hospital Ships (TAH)]. The system tracks military personnel in support of operational exercises, contingencies, and peacetime readiness missions. EMPARTS is authorized by the Chief, Bureau of Medicine and Surgery (BUMED) to ensure Navy Medicine personnel readiness and deployable administrative requirements are managed and tracked.

The Personally Identifiable Information (PII) collected includes employment information, contact information, military records, passport information, demographic information, security clearance information and medical information. Expeditionary Medicine Platform Augmentation Readiness Training System (EMPARTS) is operated and managed by the Department of Navy, Bureau of Medicine and Surgery (BUMED) Code N14.

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)

PII data is collected for verification, identification, data matching, and mission-related use. The intended use of PII is utilized to search and identify individuals hosted in the system for specific readiness status or deployable platform assignments.

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, because EMPARTS is not the initial point of 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 consent to the specific use of their PII, because EMPARTS is not the initial point of collection. Uses of PII is consistent with BUMED Policy and the System of Record Notice(s) associated with the system.

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

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. Defense Health Agency personnel providing cybersecurity support

Other DoD Components (i.e. Army, Navy, Air Force)

Specify. U.S. Navy (Budget Submitting Office (BSO)-18 Commands), U.S. Fleet Forces Command, Chief of Naval Operations (CNO) N931, and U.S. Marine Corp Headquarters personnel entering, retrieving, managing, and verifying personnel and unit readiness.

Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify.

State and Local Agencies

Specify.

Vendor: Core4ce / # N0017819D8560
Information is shared through data exchange, access to EMPARTS and per performance work statement of the contract. Appropriate Federal Acquisition Regulation (FAR) privacy and Defense Federal Acquisition Regulation (DFAR) Cybersecurity clauses are included in the contract to include requirements for Privacy 52.224-1, 52.224-2, DFARS 252.239-7001 and 252.204-7012, Refer to sections 8.2.5 and 8.4.2:

8.2.5 Handling of Personally Identifiable Information (PII)
In accordance with the Privacy Act of 1974, the contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of PII in accordance with the latest DoN policies (SECNAVINST 5211.5series). The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer Representative. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. If a contractor, including any subcontractor, is authorized access to PII, the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act.

8.4.2 Safeguards: The contractor shall protect Government information and shall be able to provide documentation (e.g., Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252.204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

x 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.

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

Databases

x Existing DoD Information Systems

Commercial Systems

Other Federal Information Systems

Medical Readiness Reporting System (MRRS), Defense Medical Human Resources System Internet (DMHRSi), Defense Manpower Data Center (DMDC), Navy Standard Integrated Personnel System (NSIPS)

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

- | | |
|----------------------------------------------------------------------------|-------------------------------------------------------|
| E-mail | Official Form (Enter Form Number(s) in the box below) |
| In-Person Contact | Paper |
| Fax | Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | Website/E-Form |
| Other (If Other, enter the information in the box below) | |

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 EDHA-11, DoD-0003

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil>
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. Unscheduled

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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 statute 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:

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 12301, Reserve components generally; 10 U.S.C. 12302, Ready Reserve, 10 U.S.C. 12304, Selected Reserve and certain Individual Ready Reserve members; order to active duty other than during war or national emergency; 5 U.S.C. 301, Departmental Regulations; E.O. 12656, Assignment of Emergency Preparedness; E.O. 9397 (SSN) as amended; 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, Navy Periodic Health Assessment for Individual Medical Readiness; Pub. L 108-735, Section 731 Ronald Reagan National Defense Authorization Act; 10 U.S.C. 671, Members not to be assigned outside

United States before completing training; and OPNAVINST 1000.16L, (N12) Navy Total Force Manpower Policies and Procedures, June 24, 2015.
47. 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.

EMPARTS does not collect information from members of the public and does not require an OMB Control Number. Citation: DoDM 8910.01, Enclosure (3), paragraph 7.b.(2)(a) and 7.b(3). Refer to the specific source system PIA(s) for additional information regarding the OMB Control Number applicability. The PIAs are available at: <https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/asp/>