



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Medical Surveillance System (DMSS)
--

US Army Medical Command - DHP Funded System
---

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

**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
- 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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army, 10 U.S.C. 8013, Secretary of the Air Force, 10 U.S.C. 5013, Secretary of the Navy; DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Directive 6490.02, Comprehensive Health Surveillance; DoD Instruction 6490.3, Deployment Health; DoD Instruction 6485.01, Human Immunodeficiency Virus; DoD Directive 1404.10, Civilian Expeditionary Workforce, and E.O. 9397 (SSN).

**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 Defense Medical Surveillance System (DMSS) supports a systematic collection, analysis, interpretation, and reporting of standardized, population-based data for the purposes of characterizing and countering medical threats to a population's health, well-being and performance. The Armed Forces Health Surveillance Center (AFHSC), which operates the DMSS, routinely publishes summaries of notifiable diseases, trends of illnesses of special surveillance interest, and field reports describing outbreaks and case occurrences. The information is released in summary fashion on a recurring basis in the Medical Surveillance Monthly Report (MSMR), the principal vehicles for disseminating medical surveillance information of broad interest to the DoD community. Through DMSS, the Armed Forces Health Surveillance Center provides the sole link between the DoD Serum Repository (DoDSR) and other databases. The DoDSR is the largest repository of its kind in the world.

Types of personal information collected include demographic data; medical and disability information; and military and employment records.

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

The DMSS collects and utilizes the minimum personally identifying information necessary to perform authorized surveillance requirements. There is a risk of inadvertent release or unauthorized use of this information. In order to minimize these risks, extensive physical, technical and administrative controls have been implemented. These controls are addressed in Section 3 below.

**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.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

Cherokee Nations Technology Solutions/ General Dynamics Information Technology -  
Contract Language:  
Privacy and Security of Protected Health Information.  
IAW DOD 6025.18R "Department of Defense Health Information Privacy Regulation"  
the Contractor meets the definition of Business Associate. Therefore, a Business  
Associate Agreement is required to comply with both the Health Insurance Portability  
and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves  
as that agreement whereby the Contractor agrees to abide by all applicable HIPAA  
Privacy and Security requirements regarding health information as defined in this  
clause, and DOD 6025.18R, as amended.

**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 information in DMSS is not collected directly from individuals. DMSS receives information from existing electronic systems and databases.

**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 information in DMSS is not collected directly from individuals. DMSS receives information from existing electronic systems and databases.

**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 information in DMSS is not collected directly from individuals. DMSS receives information from existing electronic systems and databases.