



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Department of Defense Suicide Event Report (DoDSER) System
--

TRICARE Management Activity (TMA)
-----------------------------------

### **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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 8013, Secretary of the Air Force; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. chapter 55, Medical and Dental Care; 29 C.F.R. part 1960, Occupational Illness/Injury Reporting Guidelines for Federal Agencies; 45 C.F.R. parts 160 and 164, Health Insurance Portability and Accountability Act, General Administrative Requirements and Privacy and Security Rules; DoD 6490.02, Comprehensive Health Surveillance; AR 600-63, Army Health Promotion, Rapid Action Revision 20 Sep 09, Paragraph 4-4 Suicide Prevention and Surveillance; OPNAV Instruction 1720.4A, Suicide Prevention Program, 5.d, Reporting; AFI 44-154, Suicide and Violence Prevention Education and Training; AFPAM 44-160, The Air Force Suicide Prevention Program, XI, Epidemiological Database and Surveillance System; and E.O. 9397 (SSN), as amended.

**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.

This data system will provide integrated enterprise and survey data to be used for direct reporting of suicide events and ongoing population-based health surveillance activities. These surveillance activities include the systematic collection, analysis, interpretation, and reporting of outcome-specific data for use in planning, implementation, evaluation, and prevention of suicide behaviors within the Department of Defense. Data is collected on individuals with reportable suicide and self-harm behaviors (to include suicide attempts, self harm behaviors, and suicidal ideation). All other DoD active and reserve military personnel records collected without evidence of reportable suicide and self-harm behaviors will exist as a de-identified control group. Records are integrated from enterprise systems and created and revised by civilian and military personnel in the performance of their duties.

Personally identifiable information (PII) and protected health information (PHI) collected in the system are the type of suicide event (non-fatal suicide events), event details, location of event, residence at time of event, circumstance of death, psychological, social history, behavioral, economic, education/training history, name, Social Security Number (SSN), date of birth, gender, race/ethnic group, marital status, rank/pay grade, military service, military status, job title, service duty specialty code, duty environment/status, Unit Identification Code (UIC), permanent duty station, the major command of the permanent duty station, temporary duty station (if applicable), residence address, deployment history, use of military helping services, information regarding the individual's past military experience, medical history, medical facility, unit or military treatment facility where suicide was attempted, behavioral health provider information and form completer information.

The categories of individuals covered by the system are Department of Defense active and reserve military personnel (Air Force, Army, Navy, Marines), National Guard with reportable suicide and self-harm behaviors (to include suicide attempts, self harm behaviors, and suicidal ideation). All other DoD active and reserve military personnel records collected without evidence of reportable suicide and self-harm behaviors will exist as a de-identified control group, and are not retrievable.

SYSTEM MANAGER AND ADDRESS: Director, National Center for Telehealth and Technology (T2) Defense Centers of Excellence, 9933 West Hayes Street, OMAMC, Joint Base Lewis-McChord, Tacoma, WA 98431-1100. Ph. 253.968.2282.

The system is accessed by multiple sites world-wide. The system does not host a Web site that is accessible by the public.

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

Privacy risks are inherent in any system that collects PII. These risks includes: unauthorized disclosure of PII contained in the system through unauthorized access to the system or unauthorized alteration or destruction of the data; observation of data by unauthorized passersby via "shoulder surfing" techniques; or lax security practices on the part of a data entry user. Additionally, systems are vulnerable to attacks from outsiders, including hacking of a system, or contamination by computer viruses and other malware. To mitigate these risks, data is entered via secure socket layer (SSL) encrypted sessions. Further, data transfers from the web application to the database are encrypted and travel via SSL. Records are electronic and stored in electronic storage media. The servers that house the data are always kept in compliance with the Information Assurance Vulnerability Management (IAVM) requirements and maintain current virus definitions, updated daily. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by Common Access Cards and passwords that are changed periodically. The system automatically logs out a user if there has been no activity on the system for 30 minutes. All personnel with authorized access to the system must have appropriate Information Assurance training, Privacy Act training, and Health Insurance Portability and Accountability Act

training. Mandatory refresher of all training is required by all DoD entities annually.

**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.

**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.

Individuals will be informed that participation is voluntary and will have opportunity to object to data collection during face-to-face interviews. However, regardless of whether the individual objects, some PII data elements for the DoDSER database will be obtained from existing DoD data sources (in which case there is no collection from the individual) or else in certain circumstances where DoD 6025.18-R permits use or disclosure of PII that is protected health information without authorization by the individual. See DoD 6025.18-R, C7.1 (required by law), C7.2.3 (public health activities administered by DoD), C7.4.5 (DoD health oversight activities).

(2) If "No," state the reason why individuals cannot object.

**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.

As explained in the preceding section i, DoDSER data may be obtained without consent of individuals when in accordance with DoD 6025.18-R, or may be obtained from existing DoD database sources, including personnel, medical, and deployment screening records. In neither circumstance are individuals entitled to give or withhold their consent to specific uses of PII.

**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.

Individuals will be provided with a printed Privacy Act Statement during face-to-face interviews. An identical statement will also be on the DoDSER System web form site.