



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Infrastructure Test Center (ITC) Enclaves

US Army Medical Command - Defense Health Program (DHP) Funded Application

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.

This PIA covers the ITC Test and Development enclaves used to engineer and test systems and applications that have an approved PIA. The authorities for collecting the PII in any given system or application are enumerated in their separate PIAs.

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 Infrastructure Test Center (ITC) contains Test and Development (T&D) enclaves that are isolated laboratories designed for the express purpose of design, installation, development, and testing of operating systems, applications, and configuration settings for all DoD Military Health System (MHS) projects and initiatives prior to their full development. The DoD MHS types of projects developed in the T&D enclaves include administrative, clinical and infrastructure. The application owners are required to provide a PIA for their projects and adhere to the protections identified within the ITC lab.

The ITC enclaves are as follows:

- Zone A/B Enclaves. These enclaves consist of multiple Test and Evaluation (T&E) enclaves. The distinction between each enclave is based on function, network design, Active Directory implementation, user rights, and hardware/software platforms. Each environment independently operates with a specific set of test requirements.

- Zone A Enclave. This is a centrally controlled environment that monitors, manages, and provides operational control for the other enclaves, and acts as an over-arching Active Directory-driven, laboratory-management enclave designed to centralize the system administration and operational support of all sub-laboratory systems that comprise the T&D Enclaves. This reduces a technical risk and increases the probability of successful programs by performing final systems engineering verification and validation as it relates to user-required capabilities. It is required to ensure documentation is complete, and validation performed, prior to release of the project or imitative to the production environment.

- Zone B Enclave. This enclave provides verification and validation of the systems-engineering process and confidence that the system design solution is on track to satisfy the desired capabilities. This environment is for developing, integrating, and testing "pre-development" of hardware, commercial-off-the-shelf (COTS) and Government off-the-shelf (GOTS) applications, databases, and information systems.

The types of personal information is specific to the intent of the system or application submitted for evaluation, and may include demographic data as well as medical, employment, and educational information documented in the PIAs for those systems and applications.

This PIA updates the Developmental Test and Evaluation (DT&E) Test and Development (T&D) Enclaves PIA approved on 26 July 2012.

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

The privacy risks associated with PII are unauthorized access and unauthorized disclosure of PII. There are administrative, technical, and physical security safeguards in place to mitigate these risks. The specific security safeguards are addressed in Section 3d 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.

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 PII is collected prior to the system or application being submitted to ITC for evaluation. The ITC is solely to engineer and test systems and applications that contain PII data.

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 PII is collected prior to the system or application being submitted to ITC for evaluation. The ITC is solely to engineer and test systems and applications that contain 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.

The PII is collected prior to the system or application being submitted to ITC for evaluation. The ITC is solely to engineer and test systems and applications that contain PII.

--

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.