



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Technical Training Management System (TTMS)

United States Air Force (USAF)

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.

(1) TTMS is covered by the Defense Integrated Military Human Resources (DIMHRS) SORN <http://www.defenselink.mil/privacy/notices/osd/DPR36.html>

(2) The authority to collect this PII is 10 United States Code (USC) 8013, Secretary of the Air Force and Executive Order (EO) 9397 (Social Security Number - SSN)

Data is collected from the individual and DoD Military Services Human Resource Offices and stored electronically; is maintained in controlled government facilities. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel with a need-to-know. Access to personal data is limited to person(s) responsible for maintaining and servicing TTMS data in performance of their official duties and who are properly trained, screened and cleared for a need-to-know. Access to personal data is further restricted by the use of Common Access Card (CAC) and/or strong password, which are changed periodically according to DoD security policy. Disposition pending. Until the National Archives and Records Administration has approved the retention and disposal of these records, treat them as permanent.

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.

TTMS (version 9) is a web based information system intended to provide efficiency and productivity enhancements to AETC, subordinate Technical Training Wings through the prudent application of automation. The system consists of Student Management (COTS), Course Design and Development (GOTS), TTMS Upfront (COTS), Evaluations (COTS) application software, and Oracle9i Relational Database Management System (RDBMS) software hosted by Windows 2003 operating system servers.

The overall goal of TTMS is to transform the current paper dependent and manpower intensive training management system to a computer-based system. This system will reduce time spent designing, developing, delivering, evaluating, reporting, and managing training while at the same time providing better trained Air Force personnel.

TTMS data is routed through the Keesler and Lackland AFBs. In the event of failure, Keesler AFB and Lackland AFB are designated as the alternate site for each other to support the production servers. There are no development/test servers located at Lackland AFB.

TTMS is not the authoritative source for any of the PII contained in the system: Name, SSN, Drivers License, Other ID Number, Citizenship, Gender/Sex, Race/Ethnicity, Birth Date, Mailing/Home/Office Address, Place of Birth, Marital Status, Spouse Information, Child Information, Medical Data, Employment Information, Military Records, Professional Certificates, Recruit Record Information. All information is provided via system interface with MILPDS and AFRISS

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

The risk is mishandling the PII. However, the potential for mishandling of privacy information is low. Role based system access for each user is monitored by system administrators and routinely checked for requirements access. All users of the system are required to justify their access via their supervisors, and sign an acknowledge statement about the sensitivity of the data they will have access to. All system users are made aware of restrictions on secondary uses of the data by mandatory initial and refresher Privacy Act and Information Assurance training.

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.

Privacy Act information will be shared with only TTMS faculty, personnel's supervisor, Community College of the Air Force (CCAF), MILPDS and system management personnel who are granted role-based system access and have a need to know.

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.

All personal data collected is voluntarily given by the subject individual. The individual is advised that the information provided is voluntary and is aware of the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office.

(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.

Individuals can withhold their consent, but not consent to the specific uses to their PII. The information in identifiable form is necessary for tracking and validating training records and to verify individual's identity. Information will be used for record retention, information validation, and identification validation. The individual is advised that the information provided is voluntary and is aware of the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office.

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.

TTMS is not the authoritative source for PII. Information is provided for interfaces with MiLPDS and AFRISS.

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.

