PRIVACY IMPACT ASSESSMENT (PIA)

For the

TPS Enterprise CPET Application
United Stated 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** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

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 9812

☐ **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 F036 AF AETC A Student Records

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.

The authority to collect Privacy Act (PA) information is derived from Executive Order 9397, Numbering System For Federal Accounts Relating to Individual Persons; 10 United States Code (USC) 8013, Secretary of the Air Force; Air Force Instruction 36-2201, Air Force Training Program Volume 1-6.

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.

CPET is used to maintain a record of attendance and training, class standing, completion or elimination for students attending the Test pilot School. and as a source of statistical information regarding class averages, rank, standings, etc.

Information Military personnel, foreign military personnel, and civilians will provide include, but are not limited to:
SOCIAL SECURITY NUMBERS
NAMES
DATES OF BIRTH
RACE
GENDER
PAST EDUCATION
RANK
DEGREES
BRANCH OF SERVICE
COUNTRY OF ORIGIN
HOME ADDRESS
HOME PHONE NUMBER
EMAIL ADDRESS

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

Unauthorized access to the system, though unlikely, could result in disclosure of information which could lead to identity theft. Access will be limited to authorized authenticated personnel and the required use of a firewall, Secure Socket Layer protocol, authentication, and strong password protection will mitigate the risk to levels deemed acceptable. In the event that a security violation/breach occurs, an investigation and the involved activity will make every attempt to notify the impacted individuals.

The following controls are used to mitigate the risks:
a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

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. Information on the system will be shared by Administrators of the system, Instructors at TPS, Air University, as well as the Commandant and Deputy Commandant of TPS. Information will not be shared outside the Department of Defense

☐ **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. Forms that collect personal data to be maintained in this Information Technology (IT) investment contain a Privacy Act Statement, as required by 5 USC 552a(e), and in accordance with guidelines established in AFI 33-332, Privacy Act Program. This allows the individual to make an informed decision about providing the data. The statement of understanding advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection. The Air Force rules for contesting contents are published in Air Force Instruction 33-332; 32 CFR part 806b

(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.

Forms that collect personal data contain a Privacy Act Statement (PAS), as required by 5 USC 552a(e)(3), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, are provided at the time of collection allowing the individual to make an informed decision about providing the data or participating in the program. A PAS will also be available for review if the information is collected verbally.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Forms that collect personal data contain a Privacy Act Statement (PAS), as required by 5 USC 552a(e)(3), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, are provided at the time of collection allowing the individual to make an informed decision about providing the data or participating in the program. A PAS will also be available for review if the information is collected verbally. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period (if applicable), during data collection or at any time after the program is launched. If no objections are received, consent is presumed.

Individuals seeking access to information about themselves contained in this system should address written inquiries to or visit the Superintendent for PME at each Major Command, commandant at each academy or leadership school or director of personnel at each base where a school is located. Official mailing addresses are published as an appendix to the Air Force's compilation of systems of records notices.

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.