PRIVACY IMPACT ASSESSMENT (PIA)

For the

Aircrew Graduate Evaluation Program/Introductory Flight Training (AGEP/IFT)
United States Air Force

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	1770
☐	**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.

AETCI 36-2206, Aircrew Graduate Evaluation Program

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 database tracks data for all AETC aircrew graduate and undergraduate flying training, and Introductory Flight Training (IFT). The AGEP-IFT program was developed to provide gaining-unit supervisors the ability to record their ratings and comments on the effectiveness of the prior training program. The system serves as a data repository, enabling reports to be processed at any time. The AETC Aircrew Graduate Evaluation Program is part of the instructional system development (ISD) continuum and is used to ensure that graduates from AETC training courses (undergraduate and graduate students in the pipeline) meet customer requirements. It is used as a matrix for self-inspection. Data collected from supervisors on aircrew undergraduate/graduate students is used in system and syllabus review conferences to determine if any modifications need to be made to the current syllabus.
IFT is the initial Flight Screening program that is a prerequisite to Air Force pilot and navigator training. It tracks class roster information and is the initial course for the undergraduate pipeline. It is used at 19th Air Force, and Headquarters AETC.

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

There are two basic risks for AGEP/IFT: (1) risk of unauthorized access to the system, and (2) loss of the database which contains the privacy data.
To control access to the system we use various controls: restrict access to the .mil domain, only correspond with official e-mail addresses, require a user account that has right/permissions limited to minimum required, require access via a government issues common access card (CAC), link rights/permissions to the CAC identity, log activity of the CAC card, and review CAC activity for unusual activity.
We protect the database with various controls: use many of the controls listed above, as well as, encrypt the backup files on the local hard drive. For off-site backup we apply encryption during the process of copying to tape.

Data is not shared with any other systems, either inside or outside DoD.

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 entered into AGEP-IFT is not entered by the individual. A local Base Survey Administrator (BSA), typically a registrar at the training location, gathers class roster information from approved training management system local to their base, such as Training Integration Management System (TIMS) or Graduate Training Integration Management System (GTIMS) and enters the roster into AGEP-IFT.

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 entered into AGEP-IFT is not entered by the individual. A local Base Survey Administrator (BSA), typically a registrar at the training location, gathers class roster information from approved training management system local to their base, such as Training Integration Management System (TIMS) or Graduate Training Integration Management System (GTIMS) and enters the roster into AGEP-IFT.