PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air University Student Records Information System
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	2423
☐	**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 007-57-01-16-01-3143-00

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 AETC M

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. 8013, Secretary of the Air Force
Air Force Instruction 36-2201
Air Force Training Program
Air Force Instruction 36-2301
Professional Military Education; and E.O. 9397 (SSN)

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.

Air University Student Records Information System (AUSRIS). AUSRIS is a multifaceted system providing both resident education and distance learning to the Air Command and Staff College and the Air War College. AUSRIS is the heart of the ACSC On-line Master's Program (ACSC OLMP), an Air Force Chief of Staff downward directed initiative implemented nearly two years ago and accredited by the Southern Association of Colleges and Schools. There are currently 2,923 students participating in AWC and ACSC resident programs and 2,172 students enrolled in the OLMP Master's Program. AUSRIS provides management of classes, courses, grading, and student information. The system collects individuals names, social security numbers for enrollment verification, gender, home address, e-mail address, phone number, AFSC, Rank, and service component.

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

All information collected in AUSRIS is voluntarily provided by the user. A privacy act statement is provided for the users information. Any electronic communications containing personally identifying information is digitally signed.

Records are accessed by custodian of the record system and by person(s) responsible for servicing the record system in performance of their official duties and who are properly screened and cleared for need-to-know. All records in the system are attended by responsible Air Force personnel during duty hours and stored in locked facilities under constant or periodic surveillance by Air Force Security Forces during non-duty hours. Those in computer storage devices are protected by computer system software. Access to student information is controlled in AUSRIS by the assignment of user roles thus allowing access only on a need to know basis.

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. Program completion information is transferred to the Air University Registrar System (AUREPM) for updating personnel records.

☐ **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 can voluntarily not chose to input or provide personally identifying information. However, if they do choose not to provide this information, the student is denied enrollment in the PME or On-line Masters program. This occurs because Real time Broker System (RBS) uses this information to verify with the Military Personnel Center their eligibility to enroll in the program.

(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.

Current system does not provide this capability.

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.

On all screens, the following information is displayed:

This document also contains personal information that is protected by the Privacy Act of 1974 and must be safeguarded from unauthorized disclosure.

AUTHORITY: 10 U.S.C. 8013, Secretary of the Air Force; Air Force Instruction 36-2201, Air Force Training Program; Air Force Instruction 36-2301, Professional Military Education; and E.O. 9397 (SSN).

PURPOSE: To support the core functions for the administration of academic records required for graduate education, professional military education, and continuing education. The system will provide academic records that meet the requirements of academic accreditation of Air University's various educational programs.

ROUTINE USE: None

DISCLOSURE: Voluntary. However, if you fail to provide the requested information, Air War College and Air Command and Staff College will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to AUSRIS.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☒ Social Security Number (SSN)
☒ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☐ Race/Ethnicity	☒ Birth Date	☐ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal Email Address
☒ Mailing/Home Address	☐ Religious Preference	☒ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☒ Spouse Information
☒ Marital Status	☐ Biometrics	☒ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☒ Military Records
☒ Emergency Contact	☒ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.	Parents' name and address for Commandant Letters.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

All PII data collected is from new students who are enrolling in the PME Resident courses and On-Line Masters' Program. Individuals enter some requested information into the system, in addition to the Real Time Broker Service (RBS), which is DOD' s service for verifying members eligibility in DoD, populates PII information that the individual can validate or modify based on the student entering their social security number, date of birth, and last name.

(3) How will the information be collected? Indicate all that apply.

☒	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

PII data is used for identification of the individual and verification of eligibility. PII data is also used for notification and administration of school services for AWC and ACSC resident students and the On-Line Masters program.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

To track student's educational progress and completion and faculty management.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☒ **Other**

Select individuals at the Air Force Personnel Center, Air University Registrar personnel, and the Air War College/Air Command and Staff College faculty and staff; and software developers

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ **Security Guards**

☒ **Cipher Locks**

☒ **Identification Badges**

☐ **Combination Locks**

☐ **Key Cards**

☐ **Closed Circuit TV (CCTV)**

☐ **Safes**

☐ **Other**

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**

☐ **Biometrics**

☒ **Password**

☒ **Firewall**

☐ **Intrusion Detection System (IDS)**

☒ **Virtual Private Network (VPN)**

☒ **Encryption**

☒ **DoD Public Key Infrastructure Certificates**

☐ **External Certificate Authority (CA) Certificate**

☒ **Common Access Card (CAC)**

☐ **Other**

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

- ☐ **Periodic Security Audits**
- ☐ **Regular Monitoring of Users' Security Practices**
- ☒ **Methods to Ensure Only Authorized Personnel Access to PII**
- ☐ **Encryption of Backups Containing Sensitive Data**
- ☒ **Backups Secured Off-site**
- ☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☐	**Authorization to Operate (ATO)**	**Date Granted:**	
☒	**Interim Authorization to Operate (IATO)**	**Date Granted:**	17 August 2009
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection -- Is accomplished online. Individual informed of voluntary disclosure.

Use -- Is accomplished online. If there is a need to print any individual record, that record is shredded after use.

Retention -- Once verification, enrollment and course study are complete, all student records are transferred to the Air University Registrar System (AUREPM); AUREPM then transfers completed records to the Air University Academic Records system (F036 AETC M) for archiving.

Processing -- Is accomplished online. If there is a need to print any individual record, that record is shredded after use.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Once the PII information is collected, it is protected under privacy and FOUO guidelines. PII data can only be accessed by the owning user and authorized and authenticated personnel. Users are notified of PII data when accessing system.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.