



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Automated Education Management System (AFAEMS)
--

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.

10 United States Code (U.S.C.) 8013 and Executive Order (EO) 9397, delegation by: Department of Defense Directive (DoDD) 1322.88, DoDD1322.8, Voluntary Education Programs for Military Personnel, 6 January 1997, Department of Defense Instruction (DoDI) 1322.19, 3 February 1999, and DoDI Voluntary Education Programs In Overseas Areas, 9 May 1988, and DoDD 1322.16, Veterans Educational Assistance Act of 1984, 11 May 1994, and Air Force Instruction (AFI) 36-2306 Air Force Education Services Program, 16 October 2000.

**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 Air Force Automated Education Management System (AFAEMS) is an enterprise-wide, web-based application used to manage the expansive Air Force Voluntary Education and Training Program managed by Force Development Flights. This education and training portal manages an Airman's complete education and training record, the tuition assistance budget and all related processes, as well as automates all routine tasks performed by Force Development personnel.

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

The privacy risks include computer hackers, disgruntled employees and state-sponsored information warfare.

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that AFAEMS, with its extensive collection of PII, could be compromised.

Because of this possibility, appropriate security and access controls listed in this PIA are in place.

All systems are vulnerable to "insider threats". AFAEMS administrators are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to AFAEMS. These individuals have gone through extensive background and employment investigations.

**Mitigation:**

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 of 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 an Air Force 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.

**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.

An Airman has the option to not provide their SSN, but will be unable to participate in voluntary education programs. An Airman agrees to the release of their information to the Academic Institution (AI) by signing (either digitally or manually) the AF Form 1227, Authorization for Tuition Assistance. Member must agree to the terms and conditions in order to receive tuition assistance and validates consent using initials and signature.

(2) If "No," state the reason why individuals cannot object.

Not applicable

**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.

Primarily, the individual can withhold consent by not providing the PII. All Airman have the option to not provide their SSN, but will be unable to participate in voluntary education programs. Just as the Airman

agrees to the release of their information to the release of their information to the Academic Institution (AI) by signing (either digitally or manually) the AF Form 1227, Authorization for Tuition Assistance. Member must agree to the terms and conditions in order to receive tuition assistance and validates consent using initials and signature.

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

In accordance with AFI 33-332 Rules for Releasing Privacy Act Information Without Consent of the Subject, individual consent is not required to disseminate the data stored in the Air Force Directory Service (AFDS) System or Military Personnel Data System (MilPDS) which are the host systems for PII data for AFAEMS.

**k. What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> <b>Privacy Act Statement</b> | <input checked="" type="checkbox"/> <b>Privacy Advisory</b> |
| <input type="checkbox"/> <b>Other</b>                            | <input type="checkbox"/> <b>None</b>                        |

Describe each applicable format.

The requester shows and, upon request, gives the affected individual a Privacy Act Statement for each form, format, or form letter used to collect personal data before asking for the information. The statement is delivered in electronic format.

**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.**























