



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Technical Integration Management System (TIMS)
--

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
- 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 USC 8013, Secretary of the Air Force: powers and duties, delegation by Air Education and Training Command Regulations: AETCI 36-2205 Formal Aircrew Training Administration and management, AETCI 36-2220 Academic Training, AETCI 36-2223 Flying Training Student Information Management; and Executive Order 9397.

**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.

JPATS GBTS TIMS manages all aspects of Joint Air Force and Navy primary aircraft student training. Provides scheduling of all resources-students, instructors, classrooms, classroom equipment and resource files, aircrew training (simulator) devices, aircraft, and airspace. Maintains data and provides performance evaluation and deficiency tracking of students.  
Manages syllabi and evaluates training course content. Monitors student performance by source of entry, education level, and minority status. Maintains background information and qualifications of graduates for follow-on training to Air National Guard/Air Force Reserve and other Air Force/Navy training units. Provides data for and documents proceedings in the event of Training Review Board actions. Maintains data and tracks the training, and qualifications of instructor pilots and other training cadre.

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

Privacy risks considered were unauthorized access to the server and associated database and protection of information in identifiable form, and disclosure of an individual's SSN/PII other than individuals with a need to know.

- In response to unauthorized access the application and its associated components: The servers and computer components are housed in offices, in training classrooms and in laboratories within buildings only accessible only by authorized Common Access Card (CAC) access. Server software is updated and maintained in accordance with AF standards and security mandates and evaluated to correct DoD defined vulnerabilities-all Information Assurance Vulnerability Alert (IA V A) and Notices to Airmen (NOT AM) distributed by DoD are implemented within the assigned timeframe.
- To respond to protection and disclosure of a SSN/PII, efforts are taken to insure only certain individual in application defined roles with a need to know were given access to the individual's full Social Security number - the individual, the individual's supervisor, and the security manager. The supervisor provides validation of individual information and is the first level of acceptance in granting access to a system or application. The security manager requires the full Social Security number to check Joint Personnel Adjudication System (JPAS) for security clearance and the adjudication of the individual requesting access.

**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.

- Base level - Uses system data to ensure training efficiency, identify training resource requirements, and track flying data.
- Major Command (AETC) - Uses all system data to measure the effectiveness of subordinate unit training programs and to check command-wide flying training effectiveness.
- HQ USAF- Uses various identification and flying data to establish statistical data needed to verify the effectiveness of standard procedures, determine the need for policy modification, provide a timely and accurate census of various types of flyers and jumpers and provide a centralized point for collection and collection of data used by all levels of management.

**Other DoD Components.**

Specify. US Navy - Chief of Naval Air Training (CNATRA) - TIMS is a joint program with the USN, information pertaining to Navy students training with AETC is passed back to their parent command.

**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.

The Air Force rules for accessing records, contesting contents, and appealing initial agency determinations are published in Air Force Instruction 33-332, Privacy Act Program; 32 Code of Federal Regulations (CFR) part 806b -Air Force Privacy Act program, or it may be obtained from the system manager.

(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.

The Air Force rules for accessing records, contesting contents, and appealing initial agency determinations are published in Air Force Instruction 33-332, Privacy Act Program; 32 Code of Federal Regulations (CFR) part 806b -Air Force Privacy Act program, or it may be obtained from the system manager.

(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.

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

Describe each applicable format.

Student grade folders retrieved by name can be either in the format of a soft or hard copy of information depending on what format they get the data in. If DOD and USAF forms are used, they will have the Privacy Act Statement posted in the header. These forms are provided to the recipient and collected in the same manner.





















