



PRIVACY IMPACT ASSESSMENT (PIA)

For the

FITNESS MANAGEMENT SYSTEMS (AFFMS)

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
- 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.

Authority

10 United States Code (USC) 8013, Secretary of the Air Force: powers and duties; delegation by; as implemented by Air Force Instruction 40-501; and E.O. 9397 (SSN)

Purpose

To document individuals' progress in the Air Force Fitness Program. The file keeps individuals informed of their fitness levels and of progress in improving fitness levels and achieving minimum Air Force fitness standards.

Routine uses

In addition to those disclosures generally permitted under 5 U.S.C. 522a(b) of Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The "Blanket Routine Uses" published at the beginning of the Air Force's compilation of records notices apply to this system.

Disclosure-Mandatory

Individuals who do not use AFFMS to input and maintain their scores can be subject to administrative

action or punishment.

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 Fitness Management System (AFFMS) is an Air Force wide data system acquiring and maintaining airmen physical fitness data. This system tracks all airmen's fitness test records, provides unit fitness managers management reports to facilitating the administration of the Air Force Physical Fitness Program and provide airmen the ability to see their past fitness records as well as evaluate their current physical fitness. The AFFMS provides real time access to fitness data as well as fitness management report to MAJCOM, Unit and Installation Commanders.

Specific privileges to enter data, view, retrieve and print reports, conduct audits, and correct data entries are granted according to roles and responsibilities for FP data management. Roles and responsibilities are defined by the functional consultants and granted by the system administrator. The AFFMS is currently in the sustainment lifecycle phase. The servers on which the AFFMS resides are located at Gunter Annex, Maxwell AFB, Alabama.

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

The potential to the AFFMS privacy risks regarding the collection, use, and sharing of the information in identifiable form are from internal sources. Access to AFFMS is restricted to individuals and those in the UFPM, FIM, HAWC, or commander roles who log on using their CAC/PIN combination. The individuals who also have roles as UFPM, FIM, HAWC, or commander have access to names and Social Security Numbers (SSN) of individuals under their span of control. To limit this potential privacy risk, the AFFMS only displays the last four numbers of an individual's SSN.

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.

One-way interchange of data from AFCHIPS to AFFMS. The Air Force Medical Operations Agency (AFMOA) will have read-only access to the AFFMS data to conduct Air Force Surgeon General-directed studies.

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.

Individuals do not have any opportunity to object to the collection of information in identifiable form about themselves or consent to the specific use of the information in identifiable form. AFFMS is used to track and maintain the fitness scores of individuals in accordance with Air Force Instruction 10-248. The AFFMS use is tracked by unit commanders. Individuals who do not use AFFMS to input and maintain their scores can be subject to administrative action or punishment.

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.

Individuals do not have any opportunity to object to the collection of information in identifiable form about themselves or consent to the specific use of the information in identifiable form. AFFMS is used to track and maintain the fitness scores of individuals in accordance with Air Force Instruction 10-248. The AFFMS use is tracked by unit commanders. Individuals who do not use AFFMS to input and maintain their scores can be

subject to administrative action or punishment.

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.

The AFFMS collects personal information covered by the Privacy Act. When personal information is collected for use within the AFFMS, a Privacy Act Statement or Advisory is provided on the web-based application used to collect the information.

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.

