



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Library Information System (AFLIS)
--

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.

Title 10 United States Code (USC) 8013

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 Library Information System (AFLIS) is comprised of 10 modules. Each module performs a different task related to AF Libraries. AFLIS serves the AF Library staff and is owned by the AF Library Division. AFLIS is currently in sustainment mode. AFLIS system resides in the AFSVA domain of the AFPC enclave, which resides in the Randolph network infrastructure. AFLIS is comprised of 2 servers, one web and one SQL server. Backups of the SQL data occurs every 4 hours.
The program manager of AFLIS is Debbie Meyers, DSN 487-3037, email Debbie.meyers@us.af.mil.

AFLIS provides e-ordering, order tracking/receiving, statistical reporting..... The Library Electronic Ordering Module (LEOS) performs e-ordering, order tracking/receiving, fund checking and various reporting capability. The Library Annual Report Program (LARP) module collects statistical information from all Air Force Libraries and provides statistical reports for the Congressional Hearings. Office Management Module (OCMAN) provides the libraries with a way to manage their borrowing office account items. Detailed reporting capability on office account items. These three modules out of the ten modules that comprise AFLIS agate data in such a way that some reports produced and used by government staff only contain privacy act information. The privacy act information contain in these reports include name and unit address for overseas bases and could contain points of contact for base personnel at various offices.

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

Certification and Accreditation of the system revealed few security risks – medium and low risks were considered acceptable. Because access to all data requires authentication, it guarantees proper credentials for viewing/transferring any data. The data stored in the system are transferred via HTTPS using approved DoD encryption methodologies, including the DoD PKI (e.g., Common Access Cards-CAC).

In accordance with AFI 33-332, Privacy Act Program 12.4 Rules for Releasing Privacy Act Information without Consent of the Subject, individual consent is not required to disseminate the data stored in AFLIS.

For purchasing government products from vendors who require a point of contact as well as a unit mailing address a voluntary release of name and unit address is required.

During the Certification and Accreditation process of AFLIS, (7) residual risks were discovered. Of these, (2) were rated as medium and (5) were rated as Low. The medium vulnerabilities are acceptable risk.

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.

AFLIS Leos module reports and input screen that collect or report privacy act data are shared only with AF AFLIS users. AFLIS LARP module data is shared with only AF personnel. The OCMAN module data in AFLIS is shared only with AF Library personnel. Information Assurance and Privacy Act training is an annual requirement for all AF personnel. AFLIS engineers have complete access to the data in the system in order to resolve data conflicts and resolve technical complications.

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.

Order data sent to a third party outside government. The persons name is removed before the order is sent but the ship to address is on the orders.

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.

A person can refuse to provide personally identifiable information for AFLIS by not filling out the AFLIS access request form, or the DD 2875 form or by being appointed as the point of contact for an office account. A consent form is signed by the person acknowledging the information collected is voluntary.

In compliance with AFI 33-332, Privacy Act Program, paragraph 12.4.1, any data released without consent of the subject are required in the performance of official duties.

Air Force Privacy Act complaints process rules for accessing records, for contesting contents and for appealing initial agency determinations are published in AFI 33-332, Privacy Act Program, paragraph 1.3, Privacy Act Complaints; or they may be obtained from the system manager.

In accordance with AFI 33-332, Privacy Act Program, paragraph 12.4, Rules for Releasing Privacy Act Information without Consent of the Subject, individual consent is not required to disseminate the data stored in the AFLIS system.

Exception 1 (DoD employees have sign a release. Releasing their name, email address and unit address to a non government entity for the purpose of receiving a product purchased for the Government at their request.

-- All personal data collected is voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT investment contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

-- The subject individual initiates the collection and maintenance of his/her information for the purpose of having orders placed for items on their behalf. Release of this information is done with the individual's full cooperation and consent.

(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.

A person can refuse to provide personally identifiable information for AFLIS by not filling out the AFLIS access request form, or the DD 2875 form or by being appointed as the point of contact for an office account. A consent form is signed by the person acknowledging the information collected is voluntary.

In compliance with AFI 33-332, Privacy Act Program, paragraph 12.4.1, any data released without consent of the subject are required in the performance of official duties.

Air Force Privacy Act complaints process rules for accessing records, for contesting contents and for appealing initial agency determinations are published in AFI 33-332, Privacy Act Program, paragraph 1.3, Privacy Act Complaints; or they may be obtained from the system manager.

In accordance with AFI 33-332, Privacy Act Program, paragraph 12.4, Rules for Releasing Privacy Act Information without Consent of the Subject, individual consent is not required to disseminate the data stored in the AFLIS system.

Exception 1 (DoD employees have sign a release. Releasing their name, email address and unit address to a non government entity for the purpose of receiving a product purchased for the Government at their request.

-- All personal data collected is voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT investment contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

-- The subject individual initiates the collection and maintenance of his/her information for the purpose of having orders placed for items on their behalf. Release of this information is done with the individual's full cooperation and consent.

(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"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

AFLIS Access request Forms that collect personal data will contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. All AFLIS input screens that require the Privacy Act Statement has it on the bottom of the screen as well as any reports generated that contain Privacy Act Data. Only AFLIS users are allowed to access data contained in AFLIS. Users who are office points of contact can contact the AFLIS administrator to gain information contained on them in AFLIS. The following information is collected and maintained by AFLIS: Name and Unit Address.

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.

