



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Financial Management WorkFlow (FM Workflow)

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 U.S.C. 8013, Secretary of the Air Force and Executive Order 9397 (SSN).
10 U.S.C. 8032, The Air Staff, general duties
DoD Financial Management Regulation 7000.14-R; Volume 7A, Military Pay Policy and Procedures – Active Duty and Reserve Pay
The Joint Federal Travel Regulations, Volume 1, Uniformed Service Members
The Joint Travel Regulations, Volume 2, Civilian Personnel; Air Force Instruction 65-114
Travel–Policy and Procedures For Financial Services Offices and Finance Offices-Reserve Component
Air Force Manual 65-116 V2
Defense Joint Military Pay System Active Component (DJMS-AC) Unit Procedures Excluding Financial Services Office.
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the 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 (DoD) 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of record system notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

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.

This system will enable the implementation of centralized records management across the Air Force Financial Service community. This system will also facilitate processing of financial transactions for the USAF including Military Pay (MilPay), Travel Pay (TDY); Retirement & Separation; Civilian Permanent Change of Station (CivPCS); Debts; and Disbursements. Service members will bring hard copy travel documents to the Financial Services Office (FSO) at their base in order to make a request for reimbursement or to request a change to their pay record. The Customer Service Technician at the base-level FSO will scan the hard copy documents into the FM Workflow system. The scanned, electronic documents from all bases will be centrally processed at the Air Force Financial Services Center (AFFSC) at Ellsworth AFB. Customer Service Technicians at the base will use the system to check the status of a service member request. The system will also be used by Call Center personnel to access financial services records to assist base Financial Services Offices and Air Force customers world-wide
SAF/FMP owns FM Workflow, POC: (P) Jeffrey Cramp, DSN 672-2226, jeffrey.cramp@wpafb.af.mil
(A) Gregory Wilson, DSN 675-8682, gregory.wilson@ellsworth.af.mil

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

System developers, database administrators, and functional managers within SAF/FMP have immediate access to the data. User access is controlled by User ID/Password or Common Access Card digital certificate for performance of their official duties. Users are assigned to a role file defining what data sources they have access to as well as any applicable data filters. The system hardware is behind the Ellsworth AFB firewalls and maintained in a secure environment requiring cipher lock access and security clearances.

This system is designed to safeguard information through roles based FOUO data access as defined by functional groups using this system. There is no user/use of data outside the DoD except for FOIA requests. All contractor personnel with access are considered DoD personnel.

There is limited use of data outside the DoD at this time and no unauthorized external access. At this time only FOIA oriented information may be publicly disclosed but not directly accessed through this system.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the 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 (DoD) 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of record system notices apply to this system.

Records are accessed by users with the appropriate profiles or roles and by persons responsible for servicing the record system in performance of their official duties.

Data is managed per established records dispensation schedules for records and through OPR data management rules associated with each application

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.

United States Air Force

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.

Ernst & Young LLP (Prime) and IBM, (Sub), in performance of contract duties. Contract requires baseline IA controls be implemented to ensure PII is safeguarded. Non-disclosures are in place for all EY employees working with FM Workflow systems.

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.

Not Applicable

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

The FM Workflow system is not the originating data source for much of the PII data collected. In compliance with AFI 33-332 paragraph 12.4.1; for the host data source for the PII data used, any data released without consent of the subject is required in the performance of official duties.

It is necessary to collect this information or the Department of the Air Force will not be able to track changes in duty station, direct military pay transactions., or ensure receipt of military pay.

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.

Not Applicable

(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 authoritative data sources for PII data for the FM Workflow System. Other information is entered by the individual.

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 checked="" type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The system or requester shows or upon request, gives the affected individual a Privacy Act Statement for each screen, 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.

