



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

SAF/FM Customer Relationship Management/CRM
---

SAF/FM CRM 1.1
----------------

### **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.

The system utilizes information that is sent from MILPDS and DCPDS through Data Feeds to provide updates on travel and pay inquiries from AF Members and their dependents. The authority to collect the information comes from 5 U.S.C. Section 301; Departmental Regulations; 37 U.S.C. Section 404, Travel and transportation allowances: general; DOD Directive 5154.29, DoD Pay and Allowances Policy and Procedures; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R, Volume 9; and E.O. 9397(SSN).

**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 purpose of the CRM system is to support Air Force members and their dependent's queries about the status and disposition of certain pay and travel expense reimbursement transactions that are being processed by the U.S. Air Force Financial Services Center (AFFSC). Information collected consists of Full Name, Person ID, SSN, Date of Birth, Rank, Date of Rank, Active Federal Service Date, Projected Rank, Duty E-mail, Organization Name, Base Name, Full Resident Address to Include City, State, and Country

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

There is a risk that unauthorized system users (insiders) could gain access to and misuse personnel data. To safeguard against this, technical, physical and administrative security procedures are being put in place at Ellsworth AFB and the RightNow Technologies (RNT) commercially hosted facility. In addition, the AFFSC CRM application incorporates business rules limiting access to privacy data in accordance with the roles and responsibilities assigned to them. These rules include enforcement of least privilege and need-to-know access controls.

**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.

Yes, customers may object, at the source of the System of Record (MilPDS, DCPDS). The CRM system will process batch data feeds from other DoD systems that collect and maintain the PII. The CRM system does not require direct entry of PII data, so individuals choosing to object would have to do so through the appropriate administrative structure. PII is required by the originating systems to enable proper compensation for salary and expense reimbursements, and is required by these systems as a condition of employment by the United States Air Force.

(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.

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

PII is only used by CRM to identify individuals (service members) who call the AFFSC Contact Center to inquire about issues with their pay or travel reimbursement. The Contact Center personnel will validate the identity of the caller in order to provide status information for the correct individual. The caller may choose not to share their information, but in this event, the Contact Center personnel will not be able to assist them.

\_\_\_\_\_

**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.

Callers will be informed that their information will be used for identity verification purposes and the data is not kept.

**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.**



















