



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Leave Request, Authorization and Tracking System (LeaveWeb)

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.

10 U.S.C. 8013, Secretary of the Air Force; implemented by Air Force Instruction 36-3003, Military Leave Program; 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 LeaveWeb program is a self-assistance program used to capture information to process leave requests for active duty Air Force military member. Members, newly assigned to a base, will go through their assigned unit to have a local LeaveWeb account established. Members will access the information system using their DoD Common Access Card (CAC) via direct or from the AF Portal. Using an online Web-based form members will fill out the appropriate information that is required for the AF Form 988, Leave Request/Authorization, initial request. After submitting initial request, the system sends an e-mail with the tracking number to the designated supervisor of the member with a link to the members request. The supervisor then has the option of approving or denying the leave request. Once approved, the system sends an e-mail to the unit leave monitor for approval and assignment of leave number. The member will receive an e-mail once a leave number has been assigned with a link to the approved form for printing to hand carry while on leave. Unit leave monitors, commanders, and Financial Services Office (FSO) have access to the system for reporting, system administration, and validation purposes. These documents are signed electronically using the DoD CAC and routed to the Defense Joint Military-Pay System (DJMS) for financial transactions in the member's military pay records.

Information captured from the member include name, Social Security Number, home address and phone, unit, leave address and emergency telephone number, leave days requested, leave days taken, leave balance, grade, and approving official's name.

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

Members information is only accessible by that member and by members given Approving Official (AO) access (only subordinate's leave information the AO is responsible for). System administrators are assigned to the system for various administrative and financial operations. These individuals are identified on DD Form 2875 and access is limited to the lowest access needed to accomplish their responsibilities. These special access levels are typically those same individuals who have access to this information in non-automated processes. Access is limited based on the hierarchical role assigned to them. The system is encrypted using SSL technology and accessible only using a Common Access Card (CAC) and PIN.

Information captured in LeaveWeb is the same as that captured in pen/ink processes. Using LeaveWeb the access to this information is better controlled and traceable than processes used external to the system.

LeaveWeb access is based on hierarchical user roles and security. The hierarchical roles are:

Finance Administrator: Can view everybody's information and requests on the base for financial systems

System Administrator: Can view everybody's information and requests on the base for system administration

System Unit Administrator: Can only view personnel's information and requests within their hierarchy (1+ units)

Unit Administrator: Can only view personnel's information and requests within their unit (1 unit only)

Member "User Level Access": Able to enable to generate/amend documents for themselves only.

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.

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

The Air Force currently identifies members by SSN for pay or leave purposes.

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.

Information may be disclosed to the Department of Justice, and to Federal, state and local or foreign law enforcement authorities for investigating or prosecuting a violation or potential violation of law; the American Red Cross for information concerning the needs of the member or dependents and relatives in emergency situations.

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.

Provided on opening screen of the application, main login menu.

Privacy Act Statement:

Authority: 10 U.S.C., Chapter 40; 37 U.S.C., Chapter 9; EO 9397, November 1943

Principal Purposes: To authorize military leave, document the start and stop of such leave; record address and telephone number where you may be contacted in case of emergency during leave; and certify leave days chargeable to you.

Routine Uses: Information may be disclosed to the Department of Justice, and to federal, state, local or foreign law enforcement authorities for investigating or prosecuting a violation or potential violation of law; the American Red Cross for information concerning the needs of the member or dependants and relatives in emergency situations.

Disclosure: Disclosure of SSN is voluntary. However, this system cannot process your leave request without your SSN, since the Air Force identifies members by SSN for pay or leave purposes.

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.

