



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Leave Log (LEAVELOG)
Army and Air National Guard

### **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.

Army Military Human Resource Records Management; AR 600-8-111, AR 600-8-10 - LEAVES AND PASSES; Air Force Instruction 36-3003, Military Leave Program

**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.

LEAVELOG is used to automate the process of military leave for all Soldiers and Airmen paid from the Defense Joint Military Pay System Active Component and Reserve Component. LEAVELOG saves thousands of man hours and ensures that Service Member leave balances are properly accounted for. Service Member digitally submit leave forms for approval by their supervisors. LEAVELOG has a complete workflow with the ability to sign leave forms using a Common Access Card. Upon completion of Leave, electronic transactions are sent to DFAS and applied to the Service Member's existing leave balance.

The PII data collected within the system includes some basic personnel data and leave information as required by DA Form 31 and AF Form 988. Example data elements include: Name, SSN, Rank, Leave Address, Dates of Leave

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

The safeguards in place to avoid privacy risks include: System resides in ARNG Readiness Enterprise Processing Center which is secured physically and technological protection to include: Army Guards, locked doors, firewalls and intrusion detection systems.

**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.

National Guard Bureau (NGB), including States, Territories, District of Columbia. Defense Finance and Accounting Service (DFAS)

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Contract Company Name(s): IIF Data Solutions, Inc., Broadleaf, Inc.  
CONTRACT EXCERPT: Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S.C. Section 552a and applicable agency rules and regulations.

The contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information, which may involve the contractor or the contractor's personnel or to which they may have access, may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at Government expense during the course of this contract are the property of the Government.

**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.

Collection of PII data is required for the system to function. SSN is currently the primary identifier that is used to process leave transactions via the systems interface with DJMS-AC and DJMSC-RC. The SSN is matched to the Service Member's personnel record to ensure Service Member is an active member of the ARNG or ANG. The DoD ID number is obtained from the Common Access Card. Use of the SSN will be phased out upon validation from DMDC and DFAS when pay systems have been updated to use the DoDID to identify individual pay accounts.

**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.

Once PII data is collected in LEAVELOG Service Members cannot opt for their information to be shared with supervisors. The LEAVELOG process follows the workflow defined in the leave and pass regulations which requires approval by the supervisor.  
PII data sent to DFAS is for the express purposes of charging the Service Member's leave and must be sent in order to adjust the leave balance.

**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 majority of information is collected the PII data from system interfaces. Service Members do input address and phone number while on leave as required.

The following information is present on the login screen of the system:  
PRIVACY ACT INFORMATION - The information access through this system is FOR OFFICIAL USE ONLY and must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974 as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal charges and/or penalties.

**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.**