



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Time Labor Management System

IMCOM G9 (FAMILY & MORALE WELFARE AND RECREATION COMMAND)

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 4016/DA00317 (Registered child of FMWR) 
- 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

A0215FMWRC

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.

July 7, 2008

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.

Statutory: 10 U.S.C. 3013, Secretary of the Army; 26 U.S.C. 6041, Information at Source; Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities; Army Regulation 215-3, Non-appropriated Fund Personnel Policy; Army Regulation 215-4, Non-appropriated Fund Contracting; Army Regulation, DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR); DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR); 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.

TLMS is the time and attendance software that Army NAF has used worldwide since 1985. It is a commercial-off-the-shelf (COTS) application. TLMS is the Army term for the software. Source time is the commercial name. Source Time version 520 is the standalone version. Source Time version 550 is the SQL network version. The software is used to collect time and attendance data either from a data collection terminal (DCT) such as a time clock, or based on employee work schedules stored in the system. It calculates employee work hours for payroll and labor management purposes.

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

The potential for identity theft and unauthorized use of the data by unauthorized personnel exists even with the security provided. The data is encrypted, access to information is controlled by User-ID and password, user transaction logs maintained and Novell security system is in place. Data is not released to any parties other than those with a business need to know based on their respective rights within the application. Additionally, the security measures in place within the security configuration of the system and on the NIPRNET, are in accordance with best practice and due diligence.

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.

The employee is provided with the Privacy Act Statement during in-processing. It is explained to the employee that without the information, the employee cannot be hired, work, or be paid.

(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 Privacy Act Statement is provided during in-processing.

(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.

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

Extracted only applicable sections from the source document where PII information was collected.

DA Form 3433-1 Supplemental Employment Application Form

AUTHORITY: Title 5, USC 301, Title 42, USC 410, and Title 10, USC sections 121 and 3013.

PRINCIPAL PURPOSE: To determine how well your education and work skills fit you for a job, and for personnel actions after employment, such as promotion, transfer, and pay and leave entitlements. We also need information on matters such as citizenship and military service to see whether you are affected by laws we must follow in deciding who may be employed.

ROUTINE USES: We must have your social security number (SSN) to keep your records straight because other people may have the same name and birth date. The SSN has been used to keep records since 1943, when Executive Order 9397 asked agencies to do so. We may also use your SSN to make requests for information about you from employers, schools, banks, and others who know you, but only where allowed by law. The information we collect by using your SSN will be used for employment purposes, and also for studies and statistics that will not identify you. We may give information from your records to appropriated federal agencies such as Department of Labor and the Equal Employment Opportunity Commission, to resolve and/or adjudicate matters falling within their jurisdiction. Records may also be disclosed to labor organizations in response to requests for names of employees and identifying information. Information we have about you may also be given to federal, state, and local agencies for checking on law violations or their lawful purposes.

DISCLOSURE: Your responses to the collection of this information are voluntary, but we cannot determine your qualifications, which is the first step toward getting the job, if you do not answer these questions.

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.