



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Transportation Financial Management System-MTMC (TFMS-M)

United States Transportation Command (TRANSCOM)

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.

Public Law 100-562, Imported Vehicle Safety Compliance Act of 1988; 5 U.S.C. 5726, Storage Expenses, Household Goods and Personal Effects; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force, 19 U.S.C. 1498, Entry Under Regulations; 37 U.S.C. 406, Travel and Transportation Allowances, Dependents, Baggage and Household Effects; Federal Acquisition Regulation (FAR); Joint Federal Travel Regulation (JTR), volumes I and II, DoD Directive 4500.9E, Transportation and Traffic Management; DoD Directive 5158.4, United States Transportation Command; DoD Instruction 450.42, DoD Transportation Reservation and Ticketing Services; DoD Regulation 4140.1, DoD Material Management Regulation; DoD Regulation 4500.9, Defense Transportation Regulation; DoD Regulation 4515.3-R, Air Transportation Eligibility.

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.

TFMS-M is the financial management system for the military Surface Deployment and Distribution Command (SDDC). The system interfaces with other systems, such as payroll, travel, disbursing, and SDDC non-core accounting support systems. TFMS improved cash management and controls over assets, reduced the time required to obtain financial information. TFMS allows SDDC and Defense Finance and Accounting Service (DFAS) to track on a daily basis cash management, answer vendor payment issues, and address customer billing questions. PII collected includes Name, Social Security Number, Gender and Date of Birth.

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

There are no additional privacy risks associated within TFMS. Access to records is limited to person(s) responsible for servicing the records in performance of their official duties and safeguards implemented in the need-to-know principle.

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.

TFMS Form 417 is used to gather PII for pay and entitlement. Individuals provide PII by completing this form. The Privacy Statement on the TFMS form 417 notifies the user that completion of the form constitutes consent, and withholding information will impact the ability of the organization to process the applicant's employment status and payment of payroll and entitlements.

The statement on the employment information (TFMS Form 417) reads as follows:
"Completion of this form constitutes consent to use of Privacy Information for payment of payroll and entitlements. Failure to provide this information will result in inability of the organization to process payment. This information is collected under the authority of DoD Financial Management Regulations and will be protected in compliance with the Privacy Act of 1974, as amended."

(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.

The purpose PII collection is for processing payroll and entitlements. TFMS Form 417 provides the following statement to the individual. "The information collected is used only for processing payroll and entitlements. Failure to provide the information, i.e., give consent, will result in an inability to process payment."

(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.

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

Describe each applicable format.

TFMS provides a statement on the TFMS Form 417, which is used to collect PII for pay and entitlement as follows, "Completion of this form constitutes consent to use of Privacy Information for payment of payroll and entitlements. Failure to provide this information will result in inability of the organization to process payment. This information is collected under the authority of DoD Financial Management Regulations and will be protected in compliance with the Privacy Act of 1974, as amended."

A Privacy advisory is given each new employee during in-processing through the Civilian Personnel Advisory Center (CPAC), an Army System. The advisory is summarized as follows: Army Civilian Personnel On-Line (CPOL) is provided as a public service for Civilian Personnel Policy. Information presented is considered public information and collected for statistical purposes. For security purposes, this service remains available to all users, software programs monitor network traffic to identify unauthorized uploads, changes, or activities that would otherwise cause damage. Except for authorized investigations, no other attempts are made to identify individual users. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration. (<http://acpol.army.mil/privacy.htm>)

All DFAS systems use the following notice: "Thank you for visiting the Defense Finance and Accounting Service website and reviewing our privacy policy. Our privacy policy is clear: we do not collect personal information unless provided by the customer we are seeking to assist. Immediately after resolving the customer's concerns, the privacy information is purged.

1. The DFAS public Web Site is provided as a public service.
2. Information presented on The DFAS public Web Site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.
3. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and will be scheduled for regular destruction in accordance with records disposition schedules governing the investigatory function of the law enforcement body.
6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act." (<http://www.dfas.mil/privacy.html>)

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.

Only Sections 1 and 2 (pages 1-6) of this PIA will be published per DoDI 5400.16.

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.