



PRIVACY IMPACT ASSESSMENT (PIA)

For the

| |
|-------------------------------------|
| Total Force Retention System (TFRS) |
|-------------------------------------|

| |
|--|
| Department of Navy - United States Marine Corps (USMC) |
|--|

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.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas
32 CFR 64.4, Management and Mobilization
DoD Dir 1215.13, Reserve Component Member Participation Policy
DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural and Manmade Disasters
CJCSM 3150.13B, Joint Reporting Structure Personnel Manual
DoD Instruction 6490.03, Deployment Health
MCMEDS: SECNAVINST 1770.3D, Management and Disposition of Incapacitation Benefits for Members of the Navy and Marine Corps Reserve Components (Renamed Line of Duty(LOD))
MCO 7220.50, Marine Corps Policy for paying Reserve Marines
E.O. 9397 (SSN), as amended.

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.

TFRS integrates workflow and information on personnel retention requirements. The purpose of the system is to track and monitor career planning for reenlistment, extension, lateral moves, overseas extensions, and special duty assignments of personnel. TFRS assists in overall recruitment goals and assignments.

The type of personal information about a Marine collected in TFRS includes: Name, SSN (full and truncated), citizenship, legal status, gender, race/ethnicity, birth date, place of birth, security clearance, spouse information, marital status, financial information, medical information, law enforcement information, military records, education information.

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

TFRS temporarily stores the full SSN in its database. However, as an added privacy measure, the system only displays the SSN when entered by the user. SSN has been replaced by DoD ID Number on reports and search features.

Until such time as the USMC's personnel systems, namely MCTFS and ODSE, utilize a new identifier for personnel such as DoD ID Number, or the system is replaced by a follow-on system, TFRS will require the use of SSNs as the unique identifier. Current plans are for all manpower systems that interface with MCTFS and ODSE to implement DoD ID Number within one year of MCTFS and ODSE's implementation anticipated to be during the 4th quarter FY13.

As with many information technology systems, TFRS has potential privacy risks in the areas of identity theft, unsolicited marketing, loss of customer faith in protecting their information, and compromise of sensitive information. However, potential privacy risks are mitigated through access restrictions, user roles and permissions, and annual Privacy and PII training.

Personally Identifiable Information (PII) is not shared or released to any individual, business, organization, entity, or agency outside those exclusively listed in Section 2, paragraph h below. Only those users with the Administrator role are able to provide access to TFRS. Access to TFRS is provided on a need to know basis and via a valid Public Key Infrastructure (PKI) enable authentication. All TFRS users (to include contractors) receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in TFRS. In addition, contractors receive an annual security briefing conducted by their companies Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions for safe handling procedures cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

TFRS is used exclusively by authorized Marines and contractors supporting the Marine Corps. TFRS is vulnerable to privacy threats such as environmental effects, paper to digital conversion, information warfare, sabotage, disposition and destruction of paper files, or localized disruptions caused by physical attacks and destruction as well as records loss or unauthorized update/modification of records in the system. Physical access to the TFRS servers is controlled by M&RA personnel.

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.

Contractors sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information.

Specific language in the contract is described as:

Security measures shall be taken to satisfy the security requirements in accordance with the Marine Corps System Security Plan. TFRS data/information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management.

Only contractors who have a valid need to know and a favorably adjudicated background investigation are permitted to have access to TFRS. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD.

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.

PII is not collected directly from the individual.

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 not collected directly from the individual.

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.

PII is not collected directly from the individual.

| |
|--|
| |
|--|

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.