



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Force Administration System (TFAS) Secure Personnel Accountability (SPA) Module
--

United States Marine Corps

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
- 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.

Executive Order 9397 of 23 November 1943, allows a federal department to utilize Social Security Numbers as account numbers for individual persons;
CJCSM 3150.13B Joint Reporting Structure – Personnel Manual;
DOD Instruction 6490.03, "Deployment Health," August 11, 2006;
Under Secretary of Defense (USD) Personnel and Readiness Memo to the Assistant Commandant of the Marine Corps, "Reporting of Personnel Data Supporting Contingencies and In-Theater Locations," dated 10 Apr 2003
Title 10 US Code, Section 1074f, Medical Tracking System for Members Deployed Overseas;
Title 10 US Code, 5013 Secretary of the Navy; and
Title 10 US Code 5041, Headquarters, Marine Corps

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 TFAS SPA Module provides capability in three primary functions.

Generalized Accountability: The SPA module provides real time accountability of deployed service members by allowing users to document and store, for historical purposes, daily individual location data by DoD Latitude and Longitude, Military Grid System, and Common Name. This accountability data will be documented for the purpose of improving the Office of Secretary Defense (OSD) Health Services data collection.

Joint and Unit Reporting: The SPA Module allows combatant commanders the ability to manage and deliver required accountability taskings from OSD to include the Joint Personnel Strength Report (JPERSTAT) and unit Personnel Status Report (PERSTAT).

Commander Accountability: The SPA Module allows combatant commanders the ability to manage and deliver required accountability management of present combat strength for use by the commander and his staff.

TFAS SPA Module will contain individual Marine personnel data to include: name, rank, Social Security Number (SSN), Military Occupational Specialty (MOS), gender, End of Active Service, Component Code, deployment status data, unit assignment data, and physical location data. This Personally Identifiable Information (PII) is pulled from Operational Data Store Enterprise (ODSE), Defense Management Data Center (DMDC), and user input and will be retained in the system from the time the Marine first deploys until separation from the Marine Corps.

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

Identity theft and the ability to track individuals is a potential privacy risk for the SPA module if the information within SPA is inappropriately accessed or shared.

Further, inappropriate information dissemination may compromise operational privacy and security by divulging a detailed history of the locations an individual has worked.

Additionally, the risks to the SPA Module are identical to the threat facing all networked Automated Information Systems (AIS) or applications whether government or commercial, classified or unclassified. Vulnerabilities exist in hardware and infrastructure, applications and system software, system and network management, and in the nature of humans and organizations. Several threat agents act without being directed to specific targets and are therefore threats to the TFAS SPA Module regardless of whether it is specifically targeted or not. The following are examples of these threats:

- The Human Intentional (Insider, outsider) threat to the TFAS SPA Module includes system developers, users, and maintainers; it encompasses all phases of the system life cycle. This threat agent can use tactics such as the introduction of malicious logic into the TFAS SPA Module software (application, database, or operating system).
- The Human unintentional threats (uninformed users, programmer errors, user errors) are driven primarily by the lack of experience, proper documentation and training.
- Site-specific environmental threats (power failures, outages, spikes, brownouts, loss of communications, water damage from flooding, fire) may pose a significant threat to the TFAS SPA Module.
- Intentional or unintentional inappropriate dissemination or unauthorized disclosure of TFAS SPA PII.

TFAS has taken steps to mitigate the privacy risks by implementing standardized security controls and minimizing the amount of information collected to the minimum necessary. The TFAS SPA Module has implemented all applicable controls from DoD Instruction 8500.2 based on a Mission Assurance Category (MAC) III Sensitive system. TFAS SPA Module is also controlled by a Configuration Control Board (CCB), which reviews the impact of changes on

the security posture and if risks or vulnerabilities are identified, they are mitigated immediately. Access to the TFAS SPA Module is provided on a need to know basis and via a stringent password and user name. Access to SPA data is granted at the unit level. A SPA user only has access to personnel data of the personnel that are affiliated with a unit that the user has access to based on assigned roles and permissions. Full SSNs are not viewable in the SPA; when SSNs are viewed in the SPA, only the last four digits of the SSN are viewable.

The system's security is built around privileges. Administrators have the ability to create roles by combining these privileges. Users are assigned one roles and the system uses the privileges assigned to the roles to grant access to system functions. Connections to the system are secured by 128-bit Secure Socket Layer (SSL).

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.

PII is sent to SPA from MCTFS via the ODSE. Individual Marines have the opportunity to object to PII resident in ODSE at any time. Audits are conducted to provide members the opportunity to review their PII and update it as necessary within MCTFS. Members can also view their individual record "at any time" through TFAS Marine on-Line (MOL) self-service personnel internet portal. Other individuals can ask to view or update their information "at any time" through any Installation Personnel Administration Center (IPAC). The location information and hierarchical structure are autonomously managed by SPA Module users who possess the necessary location management privileges. Using a web interface, the generated locations are used by other system users to assign to personnel. SPA Module tracks location changes to personnel records; these logs can be audited to trace a change back to a user. Once declassified, this location data updates MCTFS and ODSE and is then viewable via MOL.

(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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

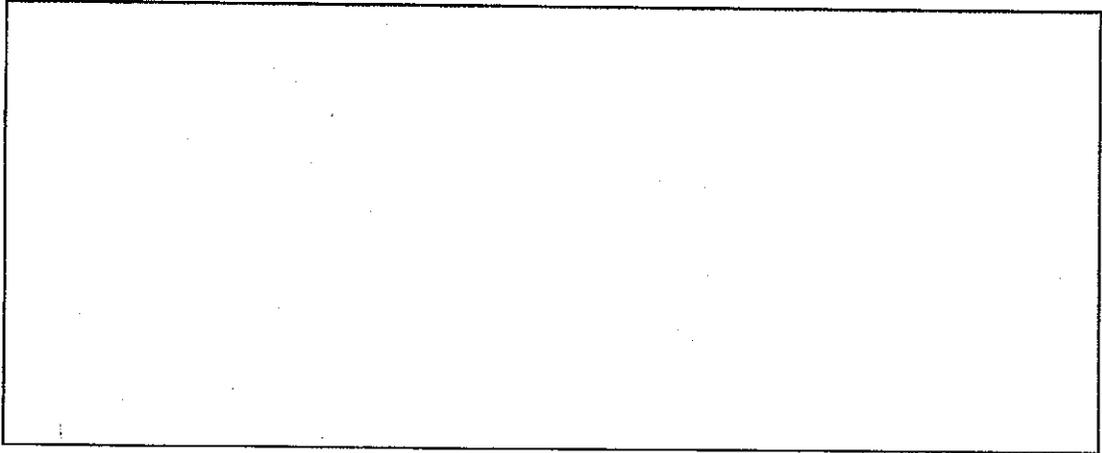
The TFAS SPA Module is used exclusively by authorized DoD personnel and any PII that is shared or released is done so with the express written permission of the individual concerned using the standard Privacy Act Statement Release Form. The TFAS SPA Module will be used in a deployed environment by personnel with the authority to manage unit personnel accountability.

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.

A Privacy Act Statement is provided and signed by all service members. The Privacy Act Statement is maintained in the member's Service Record Book (SRB), Officer Qualification Record (OQR), or civilian personnel record as appropriate.



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.