



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Force Administration System (TFAS) Drill Management Module (DMM)

Department of the 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.

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.

1. Executive Order 9397 of 23 November 1943, allows a federal department to utilize social security numbers as account numbers for individual persons;
2. Title 10 USC, Part I, Chapter 506, Section 5042, in that, the Commandant of the Marine Corps will prepare for such employment of the Marine Corps, and for such recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering, and maintaining of the Marine Corps;
3. Title 10 USC 5013, in that the Secretary of the Navy is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Navy, including the following functions: recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering (including the morale and welfare of personnel and maintaining.);
4. DoD Dir 1215.13 Reserve Component Member Participation Policy;
5. MCO 7220.50 Marine Corps Policy for Paying Reserve Marines; and
6. MCO P1001R.1J Marine Corps Reserve Administration Management Manual (MCRAMM).

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 DMM will provide Selected Marine Corps Reserve (SMCR) and Individual Mobilization Augmentees (IMAs) a web-enabled, automated means to schedule drills for Individuals or reserve units, allocate Additional Paid Drills (APDs) for Higher Headquarters and Reserve Units and muster the executed drills.

Personally Identifiable Information (PII) includes basic Reserve Marine personnel data to include, name, rank, Social Security Number (SSN), Military Occupational Specialty (MOS), and gender as well as status information that has an impact on drill capability to include eligibility to drill, record status, and strength category. Additionally, the TFAS DMM will contain information concerning scheduled drill dates and status for mustered drills. Information is collected from Operational Data Store Enterprise (ODSE) and user input.

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

TFAS DMM is used exclusively by authorized military, DoD personnel, and contractors supporting DoD. PII is shared or released only after the individual has provided written consent using the standard Privacy Act Statement Release Form. Although, the potential privacy risks within the TFAS DMM are minimal, the system is vulnerable to some privacy risks such as environmental threats, inappropriate dissemination of drill assignments, introduction of malicious logic into the TFAS DMM software, and unauthorized disclosure of PII to those without a need-to-know.

TFAS DMM will enforce the protection of sensitive data by controlling access to applications and software using identification and authentication mechanisms (e.g., user IDs and passwords or Common Access Card (CAC), discretionary access control, object reuse, and auditing. Additionally, the system is not accessible via the public internet and all SSN uses are limited to last four digit view. Furthermore, users will access TFAS DMM through a website utilizing a Security Socket Layer (SSL), 128-bit encrypted connection and role-based access will be utilized to ensure only the appropriate information is displayed to the end user based on access level.

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.

PII will be shared with the following systems and their users/owners:

System: ODSE

System Owner: Headquarters Marine Corps (HQMC), Manpower & Reserve Affairs (M&RA)

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. TFAS DMM 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 TFAS DMM. 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.

PII is sent to the TFAS DMM from 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. Members can also view their individual record through TFAS Marine On-Line (MOL) self-service personnel internet portal. Other individuals can ask to view or update their information through any Installation Personnel Administration Center (IPAC).

(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.

PII must be collected to support the Marine Corps Reserve drill management process. If an Individual were given the opportunity to withhold their consent, it would prevent leaders and administrators from having the ability to identify Marine Reservists, perform necessary drill accounting functions to include scheduling, allocating and mustering of drills, and provide subsequent personnel record updates relevant to drilling.

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

Describe each applicable format.

All Service personnel and applicants for service sign their NAVMC 11000 Privacy Act statements which are maintained in their Service Record Books (SRB) or Officer Qualification Record (OQR) and cover the collection of PII in all DoD Automated Information Systems (AIS) to manage their military careers and the Services force structures.

All TFAS DMM users receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard PII. In addition, contractors receive an annual security briefing conducted by their company's Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

The TFAS DMM specific Privacy Act Warning (PAW) pop-up screen for all TFAS DMM users to acknowledge, each and every time a user logs into TFAS DMM has been implemented in its last update. The TFAS DMM Program Manager is working with the developer to implement the TFAS DMM specific Privacy Advisory Statement (PAS) pop-up screen for users to acknowledge and provide to a Records Subject when collecting PII from a Records Subject. This PIA will be amended once the PAS is fully implemented within DMM.

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.