# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| |
|---|
| Joint Force Requirements Generator II (JFRG II) |
| 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.**

## 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 1357

☐ **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** 007-17-05-13-02-1245-00

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** M01040-3

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.

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.

Joint Force Requirements Generator II (JFRG II) is a Global Command & Control System (GCCS) approved segmented application that has been designated as the joint single source feeder system for unit movement information from the Transportation Coordinators' Automated Information for Movement System II (TC-AIMS II) and Marine Air Ground Task Force (MAGTF) Deployment Support System (MDSS II) which feed the Joint Operational Planning and Execution System (JOPES). It provides the MAGTF Commander with the automated ability to plan, coordinate, manage and execute the MAGTF operations relevant to the various phases of transportation. This application is designed to support deliberate and crisis action planning in the Force Deployment and Execution (FDP&E).

The Personally Identifiable Information (PII) information collected by JFRG II includes: Name, truncated SSN, gender, Grade/Rank, Date of Birth (DOB), blood type, address and marital status.

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

The PII data in JFRG II is inherent in the data packages that are imported from MDSS-II and TC AIMS II. JFRG II, itself, does not require any PII data to perform its designed functions and does not request or collect PII data from personnel. JFRG II designed purpose is to validate operational plan (OPLAN) requirements against the submitted data to determine if the requirements are being met. However, because there is PII within the imported data packages that are stored within the JFRG II application, minimal privacy risks do still exist that could be exploited in the form of identity theft, data corruption and internal data misuse.

Because the imported data from MDSS-II and TC-AIMS II contains PII and will be stored in JFRG II, operators and administrators will have access to view the data and existing instructions have been promulgated that provides directions to the Marine Corps JFRG users/operators on how to properly maintain, collect, use or disseminate information (Reference: SECNAV Instruction 5211.5E). The System of Records Notice Identifier (F024 AF USTRANSCOM D DoD provides the requirement that allows the collection of PII as well as the guidance for storing, retrieving, accessing, retaining and disposing of personal information. User/Operators are regularly briefed that they will be held accountable if the PII data contained in JFRG II is misused, altered or mishandled during their watch should a breach of privacy and/or identity theft occur, and that they will be subject to the articles of the UCMJ and possible civil actions. For civilian personnel, disciplinary and/or administrative actions, including dismissal and/or referral to a civil court, will be taken.

The risks involved with PII contained in JFRG II are mitigated in several ways. First, the handling of the data is done by a very limited number of JFRG II operational personnel. All JFRG II operators have, at a minimum, a secret clearance and require special training to conduct the JFRG II business processes. Second, the JFRG workstation is normally located and secured in a vault/cipher lock room in which only system administrators or qualified users can access the data if needed. Finally, monitoring of activities is overseen by senior unit 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. System: MAGTF Deployment Support System (MDSS II)
Owner: USMC

☒ **Other DoD Components.**

Specify. System: Joint Operational Planning and Execution System (JOPES)
Owner: Defense Information Systems Agency (DISA)

Transportation Coordinators' Automated Information for Movement System II (TC-AIMS II)
Owner: U.S. Army

□ **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.

(2) If "No," state the reason why individuals cannot object.

JFRG II does not request PII from individuals. All PII data used within JFRG II is imported from TC-AIMS II and MDSS II. As data is loaded from system-to-system via auto-interfaces, individuals cannot object to the collection of their PII.

**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 PII data in JFRG II is inherent in the data packages that are imported from MDSS-II and TC AIMS II. JFRG II, itself, does not require any PII data to perform its designed functions and does not request or collect PII data from personnel. Since JFRG II does not request PII from individuals, there is no requirement or opportunity for individuals to give or withhold their consent. As stated above, JFRG II does not require PII to perform its missions.

**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.

JFRG II does not require PII to perform its missions. No information is provided to the individual.

All Marine Corps personnel have a signed an OPNAV 5211/12 (Mar 1992) Privacy Act Statement (PAS) in their service jackets that can be used as required in the performance of their assigned missions.

**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.**