



PRIVACY IMPACT ASSESSMENT (PIA)

For the

OPTICAL DIGITAL IMAGING-RECORDS MANAGEMENT SYSTEM (ODI-RMS)

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-117?

- 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

M01070-6 Marine Corps Official Military Personnel Files

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.defenseink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

March 17, 2008, 73 FR 14234

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) 10 U.S.C. 5041, Headquarters, Marine Corps
- (2) 42 U.S.C. 10606 as implemented by DoD Instruction 1030.1
- (3) Victim and Witness Assistance Procedures
- (4) E.O. 9397 (SSN)
- (5) 5 U.S.C., Section 301, Departmental Regulations
- (6) MCO P1300.8R Marine Corps Assignment Policy
- (7) MCO P1070.12 Marine Corps Individual Records Administration Manual (IRAM)
- (8) 10 U.S.C. 5013, Secretary of the Navy
- (9) MCO 1610.7 Fitness Report Audit Program
- (10) MCO 1610.11A Performance Evaluation Review Board
- (11) MCO 5210.11E Marine Corps Records Management Program
- (12) MCO 5213.7C Marine Corps Forms Management Program

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.

Optical Digital Imaging-Records Management System (ODI-RMS), along with the Digital Board Room (DBR) is utilized to manage Official Military Personnel Files (OMPFs) within the United States Marine Corps (USMC). ODI-RMS was fielded in 1998 and is fully operational. ODI-RMS maintains the OMPFs used in the selection, promotion and assignment of USMC personnel. ODI-RMS is currently in the Department of Defense (DoD) Acquisition Operations and Support Phase.

The primary purpose of ODI-RMS is to support the centralized selection, promotion, retention, and assignment of Marines. ODI-RMS is the core records management system of the USMC and provides a means for storing, requesting, viewing, correcting, retiring, and temporarily loaning OMPFs. OMPFs contain performance, administrative, and award information on each Marine. ODI-RMS supports both the Active Duty and Reserve Components of the Marine Corps and provides a means for Marine Corps personnel to view their OMPF. ODI-RMS scans, index, and quality controls documents going into a Marine's OMPF folder. The server accepts documents in the form of paper and microfiche; the microfiche is scanned using a microfiche scanner where the scanning software resides. Paper records are scanned directly into a database by batches using a scanner connected to a Personal Computer (PC); after the records are in the database, paper records are shredded. A user will view and index them (determine image type, subtype, etc.) and perform quality control on the batch. On a daily basis, batches that have been indexed and quality controlled are downloaded to the Database Management System (DBMS) server for processing into the Marine's OMPF. The implementation provides an accurate update of member records, as well as access to these records for authorized users in a timely and accurate fashion. All ODI-RMS users are located within Marine Corps Base (MCB) Quantico, Virginia (VA). In addition there are MMSB personnel who are located in St. Louis, Missouri (MO) and access ODI-RMS via a Navy and Marine Corps Intranet (NMCI) connection.

ODI-RMS interfaces with PES and DBR. PES is a file server used by ODI-RMS users to access all ODI-RMS and PES applications which, provides for periodic reporting, recording, and analysis of the performance and professional character of Marine's in the grades of Sergeant through Major General. Its fundamental concepts are accuracy, accountability, simplicity, and consistency of policy and evaluation methods. The information technology capability of PES allows for creating, scanning, and processing of fitness reports that are then made part of the Marine's OMPF in ODI-RMS and provide the data necessary for selection used in DBR. DBR is an application that provides selection board members the capability to build cases, review records, and vote for selection in a secure environment. DBR displays and views OMPFs for Marine Corps promotion and selection boards. The DBR application uses digital OMPFs residing at the Manpower and Reserve Affairs (M&RA), Manpower Management Support Branch (MMSB) at Quantico, Virginia.

The type of personal information about a Marine collected in ODI-RMS includes: Rank, Social Security Number (SSN), Military Occupational Specialty (MOS), gender, religion, home address, unit name and address, date of rank, future duty station name and address, home of record address or other additional address if taking leave en route to the new duty station. Backup of data will be accomplished using a daily disk-to-disk copy with a weekly backup to storage tapes.

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

ODI-RMS is used exclusively by authorized military, DoD personnel, and contractors supporting DoD. Personally Identifiable Information (PII) is shared or released only after the individual has provided written consent using the standard Privacy Act Statement Release Form. ODI-RMS 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. Only those users with the Administrator role are able to provide access to the ODI-RMS application. Physical access to the servers is controlled by MMSB 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.

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

System: Performance Evaluation System (PES)
System Owner: Manpower and Reserve Affairs (M&RA).

System: Operational Data Store Enterprise (ODSE)
System Owner: USMC M&RA.

System: Digital Board Room (DBR)
System Owner: Administrative and Resource Information (ARI) branch of M&RA

System: Official Military Personnel Files (OMPFs) Plus
System Owner: USMC M&RA

Other DoD Components.

Specify.

System: Defense Personnel Records Information System (DPRIS)
System Owner: Personnel and Readiness Information Management Office (PR&IM) Office of Under Secretary of Defense for Personnel Readiness (OUSD)

System: Department of Veterans Affairs (DVA)
System Owner: Compensation and Pension Service (C&PS), Veterans Benefit Administration (VBA)

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. ODI-RMS 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 ODI-RMS. During the

course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD. A Top Secret clearance will be required for personnel requiring access to Defense Enterprise Computing Center (DECC) St. Louis, MO.

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 directly entered into ODI-RMS by users. ODI-RMS receives PII from PES, OMPF Plus, as well as Marine Corps Total Force System (MCTFS) through its interface with ODSE. The opportunity to object to PII is provided to the civilian applicants for entrance into the Marine Corps and individual Marines when being collected in MCTFS, PES and OMPF Plus. Failure to provide PII at time of collection in one of these three systems would prevent the individual from being accepted into the Marine Corps. It would also prevent the Marine from being considered for promotions and make them ineligible for world-wide-deployment or assignment and the Marine would have to be discharged from the Marine Corps.

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.

There are no specific uses of PII resident in ODI-RMS outside the purpose of the system to support the centralized selection, promotion, retention, and assignments of Marine's. Although Marine's do not have the opportunity to object to PII within ODI-RMS, they do have the opportunity to object to information in MCTFS at anytime. An annual audit of MCTFS is conducted to give members the opportunity to review their

information and update it as necessary. A Marine can also view their individual record through the Total Force Administration System (TFAS) Marine OnLine (MOL) application which is a self-service personnel portal.

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.

All official ODI-RMS users receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard PII. In addition, contractors who have access to the system also receive an annual security briefing conducted by their companies 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.

All official ODI-RMS users are required to read and acknowledge a Privacy Act Warning (PAW) which notifies the official user that they are entering into a system that is governed by rule-making established by the Privacy Act of 1974 [5 U.S.C. 552a] and that mandated safeguarding, handling and disposal procedures must be observed. The PAW further apprises the official user that they are not allowed to share or disseminate PII from ODI-RMS unless authorized by law and that civil and /or criminal penalties will apply. However, ODI-RMS currently does not have the pop-up PAW functionality implemented. The ODI-RMS Project Officer and functional will work with the vendor to develop and implement the PAW pop-up functionality. The risk and mitigation strategy will be included in the POA&M.

Currently ODI-RMS does not collect PII directly from an individual. ODI-RMS only receives PII from those systems listed in Section 3, para (2) of this PIA. Should a future requirement to collect PII from an individual arise, the ODI-RMS Functional Manager in coordination with the Marine Corps Systems Command (MCSC) ODI-RMS Project Officer will evaluate the requirement and its associated risks to PII within ODI-RMS and ensure any known risks are mitigated through the ODI-RMS Change Control Board (CCB). Should the requirement be approved to be implemented within ODI-RMS, this PIA and its associated SORN will be updated to reflect the change in PII collection. Lastly, the PAS notification procedures and inclusion of PAS "pop-up" screens in ODI-RMS will be mandated to be implemented at the same time the functionality is implemented within ODI-RMS.

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.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

	Digitally signed by PATUBO.JEFFREY.E.1168655262 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=PATUBO.JEFFREY.E.1168655262 Date: 2009.08.25 14:47:43 -04'00'
Name:	PATUBO.JEFFREY.E.1168655262
Title:	Captain Jeffrey Patubo
Organization:	ODI-RMS Project Officer
Work Telephone Number:	MCSC Product Group (PG)-10
DSN:	703-432-5113
Email Address:	378
Date of Review:	jeffrey.patubo@usmc.mil
	25 August 2009

Other Official Signature (to be used at Component discretion)

	Digitally signed by DUBBERLY.THURMAN.C.JR.1067668606 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=DUBBERLY.THURMAN.C.JR.1067668606 Date: 2009.08.25 15:46:41 -04'00'
Name:	DUBBERLY.THURMAN. C.JR.1067668606
Title:	Mr. Thurman (Clay) Dubberly
Organization:	Information Assurance Manager (IAM)
Work Telephone Number:	Manpower and Reserve Affairs (M&RA)
DSN:	703-784-0643
Email Address:	
Date of Review:	thurman.dubberly@usmc.mil

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

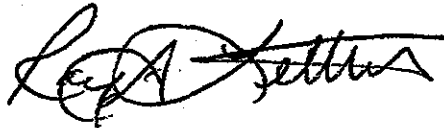
Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior
Information Assurance
Officer Signature or
Designee**



Name:

Ray A. Letteer

Title:

Chief, Information Assurance (IA) Division

Organization:

HQMC Command, Control, Communications and Computers (C4) IA

Work Telephone Number:

(703) 693-3490

DSN:

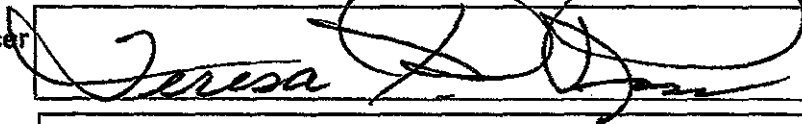
Email Address:

ray.letteer@usmc.mil

Date of Review:

11 Sep 2009

**Component Privacy Officer
Signature**



Name:

Teresa D. Ross

Title:

USMC Privacy Act/FOIA Officer

Organization:

HQMC ARSF

Work Telephone Number:

(703) 614-4008

DSN:

224-4008

Email Address:

SMBHQMCPRIVACYACT@USMC.MIL

Date of Review:

9/4/09

**Component CIO Signature
(Reviewer)**



Name: Steve Muck

Title: Privacy Team Lead

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 614-5987

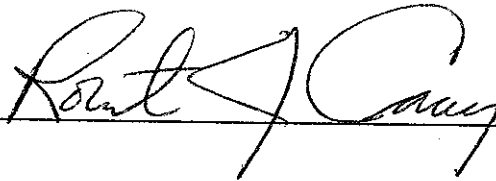
DSN: 224-5987

Email Address: steven.muck@navy.mil

Date of Review:

21 SEP 09

**Component CIO Signature
(Reviewing Official)**



Name: Robert J. Carey

Title: Chief Information Officer

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 602-1800

DSN: 332-1800

Email Address: robert.carey@navy.mil

Date of Review:

9/21/09

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.