PRIVACY IMPACT ASSESSMENT (PIA)

For the

Manpower Mobilization Assignment System (MMAS)
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	
☐	**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 MMN00013: PERSONNEL MGMT WORKING 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.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.

(1) 10 U.S.C. 5013, Secretary of the Navy
(2) 10 U.S.C. 5041, Headquarters, Marine Corps
(3) 5 U.S.C., Section 301, Departmental Regulations
(4) 32 CFR 64.4; Management and Mobilization
(5) MCO 1000.8, Fleet Assistance Program (FAP)
(6) MCO 1001.60, Pretrained Individual Manpower (PIM) Assignment Program
(7) MCO 1001.62, Individual Mobilization Augmentee (IMA) Program
(8) MCO 1300.8R Marine Corps Assignment Policy
(9) MCO 1300.31A, Enlisted Classification and Assignment Documents
(10) 10 U.S.C. 5031 Office of the Chief of Naval Operations

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 MMAS is made up of three distinct systems; Marine Corps Mobilization Processing System (MCMPS), Casualty Estimation Model (CASEST), and Force Allocation Model (FAM). The type of personal information collected in MMAS includes: Name, Rank and date of Rank, Military Occupational Specialty (MOS), gender, religion, home address, unit name and address, future duty station name and address, home of record address or other additional address if taking leave en route to the new duty station. This information is imported from the Marine Corps Operational Data Storage enterprise (ODSE).

MMAS contains the following Personal Identifiable Information (PII):
Last four of Social Security Number (SSN), Pay Grade (PGRD), Marital Status, Blood Type, Height, Weight, Eye Color, Hair Color, Security Clearance Level, and Physical Fitness Test (PFT) scores, Name, Rank and date of Rank.

MMAS optionally contains: Required Shots, Medical Examinations and Tests. These fields must be manually uploaded by an authorized MMAS user.

The primary purpose of each system and system module is listed below:

MCMPS provides support to Manpower Management Force Augmentation (MMFA) in the management of individual augmentation process as well as management of manpower activation processes of the United States Marine Corps (USMC). MCMPS consists of several integrated modules in order to properly provide required capabilities to the USMC.

The Manpower Requirements Tracking Module (MRTM) is used to request and track requirements identified by commands throughout the Marine Corps. The Processing Module is used to track the activation process of USMC Retirees and Reserve Marine's ordered to active duty. Individual Augmentation Management Module (IAMM) provides capability for all commands throughout the Marine Corps to manage Marine's that were sourced into the requirements in the MRTM.

The Billet Advertising Module (BAM) is a MCMPS module utilized to advertise open billets that need to be filled. Applicants can submit limited PII through BAM. This information is only viewable by authorized users of MCMPS and requires CAC-Enabled login. PII applicants submit through BAM include: Name; Rank; Address; Phone Number; Civilian Occupation; Email Address.

MCMPS connects to the Navy Marine Corps Mobilization Processing System (NMCMPS) via the Automated Requirements Transfer Interface (ARTI) a secure web services connection to facilitate the automatic transfer of United States Navy (USN) requirements generated within the USMC MCMPS MRTM application.

MCMPS contains the following specific elements for all members in the database (these fields are optional); Required Shots, Medical Examinations and Tests. Without this data, it would be possible to issue mobilization orders to the wrong individual or to someone not qualified for a specific billet as some billets carry strict eligibility requirements. In this case, MMAS_MCMPS may include limited medical information as described above. This medical information, if required, is entered into MCMPS by authorized users.

CASEST provides the USMC Operating Forces with an automated tool by which a user can evaluate combat scenarios and generate estimated casualty numbers for manpower planning purposes. There are two instances of CASEST in the production environment. One resides on the Secure Internet Protocol Router Network (SIPRNet), and the other on the Unclassified Marine Corps Enterprise Network (MCEN). It also enables Headquarters Marine Corps (HQMC) to develop the required manpower pool to replace anticipated casualties. The CASEST system does not contain PII.

FAM is the key tool used to identify for the USMC manpower assignment systems the allocation of units and Marine's for activation. This model organizes the competing demands for manpower into a coherent structure that can be analyzed within the confines of the allocation from the Secretary of Defense (SecDef).

FAM is a legacy system that is not currently employed to support operational needs but still could be utilized if required; FAM is a tool used if the Marine Corps units, active and reserves, deploy overseas during times of war and national emergency. FAM does not contain PII.

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

MMAS_MCMPS is a manpower system used to mobilize Marines in the Selective Marine Corps Reserve-Individual Mobilization Augmentees (SMCR-IMA), Individual Ready Reserves (IRR) and individual retired Marine desiring to Augment. MMAS_MCMPS requires the member's full name, SSN, rank, grade, security clearance level, and physical fitness information to ensure the right individual is mobilized to the right billet. Without this data, it would be possible to issue mobilization orders to the wrong individual or to someone not qualified for a specific billet as some billets carry strict eligibility requirements. This information is acquired through the system interface with the ODSE. MMAS_MCMPS may include limited biometric and medical information. Medical information can be appended by authorized MMAS_MCMPS users if required.

MMAS_MCMPS mobilizes Marines in the Individual Ready Reserve (IRR).
IRR Marines are not issued DoD Common Access Cards (CACs). MMAS_MCMPS utilizes a Marine's MCTFS-ODSE record for personnel information. The primary identifier for Marines in this system is their service number, SSN. Personnel utilizing MMAS_MCMPS frequently need to conduct additional research on Marines in other Manpower systems including MCTFS (3270). Being that MCTFS (3270) utilizes SSNs as the primary identifier, MCMPS users require accessibility to SSNs.

As a privacy measure, while MMAS_MCMPS stores the full SSN in its database, the system displays only the last four digits of a Marine's SSN in all system views and reports. Until such time the USMC's personnel systems, namely MCTFS-ODSE, utilize a new identifier for personnel such as EDI-PI, MMAS_MCMPS will need to use SSNs as the unique identifier.

The data contained in MMAS is exposed to privacy threats such as; identity theft, sabotage, and information warfare. To provide a layer of identity protection, MMAS displays only the last four digits of a member's SSN in system views and reports. MMAS users can still search for a member using the full SSN to ensure the correct individual is mobilized, but the information will not appear in system views and reports.

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: Operational Data Store Enterprise (ODSE)
System Owner: USMC, Manpower & Reserve Affairs (M&RA).

Future users/owner will share PII with MMAS.

System: Marine Corps Reserve Order Writing System Web-enabled (MROWS-W)
System Owner: MARFORRES; Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC)

☒ **Other DoD Components.**

Specify.

System: Navy Marine Corps Mobilization Processing System (NMCMPS)
System Owner: United States Navy (USN), Navy Personnel Command (PERS-46), 5720 Integrity Drive, Millington, TN 38055-3120

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Contractors have access to privacy data and are bound to the Privacy Act by the terms of the contract. They agree to abide by the Privacy Act of 1974.

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. MMAS 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 MMAS. 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.

MMAS information is not solicited directly from individual record subjects. Instead, information is populated into MMAS from other records sources (of validated integrity). The ability to object or not object is facilitated through the initial collection of information directly from the individual record subject, such as MCTFS, SRBs/ OQRs, etc.). Individuals can only change information present in MCTFS – they cannot object to the collection. 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 Total Force Administration System (TFAS) Marine On-Line (MOL) self-service personnel internet portal or by visiting their Installation Personnel Administration Center (IPAC).

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.

As data is shared from the centralized manpower databases (ODSE and MCTFS), individuals are not provided the opportunity to object to the data collection. Although Marines do not have the opportunity to object to PII within MMAS, 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 MMAS 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 MMAS users must read and acknowledge the 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 MMAS unless authorized by law and that civil and /or criminal penalties will apply. However, MMAS currently does not have the pop-up PAW functionality implemented. The MMAS 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.

MMAS receives PII from those systems listed in Section 3, para (2) of this PIA and by upload by authorized users. Should a future requirement to collect additional PII arise, the MMAS Functional Manager in coordination with the Marine Corps Systems Command (MCSC) MMAS Project Officer will evaluate the requirement and its associated risks to PII within MMAS and ensure any known risks are mitigated through the MMAS Change Control Board (CCB). Should the requirement be approved to be implemented within MMAS, 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 MMAS will be mandated to be implemented at the same time the functionality is implemented within MMAS.

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 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☒ Other Names Used	☒
☒	☐	☐
☒	☐	☒
☒	☒	☒
☐	☒	☒
☒	☒	☒
☐	☐	☐
☒	☐	☐
☐	☒	☒
☐	☐	☒
☒	☒	☐

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

MMAS receives PII through system-to-system as well as interfaces with the M&RA Manpower Portal via a web service over Hyper Text Transfer Protocol Secure (HTTPS). The interface between MMAS and the Manpower Portal is used for Public Key Infrastructure (PKI) authentication of users. The primary source of data for MCMPS will be individual service member including IRR member record retrieved from the Operational Data Store Enterprise (ODSE). Additionally, limited medical information can be appended to the system by authorized users. This information is used to ensure members have been properly screened when making assignment/mobilization decisions.

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☒	**Other**		

Medical information can be manually uploaded by authorized MCMPS users if required.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

The PII stored in MMAS is used to automate the reserve mobilization order writing process. In order to accomplish this, MMAS must have access to the PII data elements required to write mobilization orders for Marines.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

PII is used within MMAS to provide an automated and integrated method to access information essential for making mobilization assignment and career management decisions for individual augmentees and reservists. This system also allows official users to perform ad-hoc and “canned” queries for meeting higher headquarters reporting requirements. MMAS_MCMPS is used to support the creation of mobilization orders for individual augmentees and reservists.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☒	**Yes**	☐	**No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

MMAS will aggregate PII along with Marine Corps Staffing Goal data from the systems and applications listed in Section 2.h above to satisfy assignment goals and staffing for our Marine Corps Commands. Risks will be mitigated through use of CAC authenticated accounts and DOD mandated privacy act training (Information Assurance, PII, etc), in addition to hardware and software security. MMAS will modify a Marine's data record folder with updated information and allow the user to store and make available that data to servers, applications and systems for more accurate analysis and to meet reporting requirements.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☐ **Developers** ☐ **System Administrators** ☒ **Contractors**

☐ **Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ **Security Guards**	☒ **Cipher Locks**
☒ **Identification Badges**	☐ **Combination Locks**
☐ **Key Cards**	☐ **Closed Circuit TV (CCTV)**
☒ **Safes**	☒ **Other**

The MMAS servers are located in the accredited Manpower Systems enclave managed by Manpower Information Technology (MIT) at the Marsh Center, MCB Quantico. The servers are housed in a secure server room with a cipher lock on the door. All individuals entering the server room must be approved by MIT's Division Head. Additionally, system back-ups are stored in approved safes located at the Marsh Center, MCB Quantico.

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**	☐ **Biometrics**
☒ **Password**	☒ **Firewall**
☐ **Intrusion Detection System (IDS)**	☐ **Virtual Private Network (VPN)**
☒ **Encryption**	☒ **DoD Public Key Infrastructure Certificates**
☐ **External Certificate Authority (CA) Certificate**	☒ **Common Access Card (CAC)**
☐ **Other**	

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☐ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	3 Nov 08
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

PII is collected using system-to-system interfaces and manual upload by authorized users with data integrity protections in place. All encryption devices comply with the requirements of Department of Defense Directive (DoDD) 5200.5, Federal Information Processing Standard (FIPS) 140.1 and/or DoD PKI initiatives. All Communication Security (COMSEC) will be handled in accordance with COMSEC Material System (CMS)-21. MMAS is required to be PKI enabled to protect the transmission of personal information.

Information is protected by security controls and processes from the time it is entered in MMAS until it is retired. The electronic data is stored on hardware that is physically protected by cipher locked doors, limited access by authorized personnel, and access controlled during normal and after hours. The processing of documents into MMAS is controlled through the Privacy Act and the rules and regulations covering PII. Documents received electronically are protected by the means in which the data is transferred, primarily through secure e-mail or through secure file transfer protocol (SFTP).

MMAS is 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.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

MMAS_MCMPS employs several measures to address privacy risks and protect PII. MCMPS uses role based access control and users are authenticated with their DoD CAC. This method ensures only authorized users, with a need to know, are able to access the system data. Additionally, by combining CAC authentication and action logging, MCMPS enforces non-repudiation. This allows system administrators to accurately track user activity and determine if users are uploading unauthorized PII. Upon accessing the system, and prior to uploading attachments, MMAS_MCMPS warns users about the legal ramifications and dangers of misusing or inappropriately handling of PII. Once authenticated to the system, MMAS_MCMPS displays only the last four digits of a member's SSN in system views and reports to protect this vital piece of information.

MMAS_MCMPS currently employs 128-bit encryption via Secure Socket Layer (SSL) to protect the transmission of personal information. MMAS_MCMPS does not contain any classified information. The primary measure to protect the information stored in MMAS resides in the underlying operating system security subsystem. If a server crash were to occur, a full-time database administrator will manage the server logs and identify potential problems or issues with the server. The database administrator has in place a back up and restore process that allows the application to be re-installed and configured.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

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	YOON.KIL.Y.1232073680 Digitally signed by YOON.KIL.Y.1232073680 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=YOON.KIL.Y.1232073680 Date: 2009.11.09 12:48:32 -05'00'
Title:	MMAS Project Officer
Organization:	Marine Corps System Command (MCSC) Product Group (PG)-10
Work Telephone Number:	703-432-5129
DSN:	
Email Address:	kil.yoon@usmc.mil
Date of Review:	
Other Official Signature (to be used at Component discretion)	DUBBERLY.THURMAN.C.JR.1067668606 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: 2009.11.11 16:18:18 -05'00'
Name:	Mr. Thurman (Clay) Dubberly
Title:	Information Assurance Manager (IAM)
Organization:	Manpower and Reserve Affairs (M&RA)
Work Telephone Number:	703-784-0643
DSN:	
Email Address:	thurman.dubberly@usmc.mil
Date of Review:	

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	LETTEER.RAY.A.1161853565 Digitally signed by LETTEER.RAY.A.1161853565 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=LETTEER.RAY.A.1161853565 Date: 2009.11.23 14:43:40 -05'00'
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:	
Component Privacy Officer Signature	ROSS.TERESA.D.1229719277 Digitally signed by ROSS.TERESA.D.1229719277 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=ROSS.TERESA.D.1229719277 Date: 2009.11.16 14:23:29 -05'00'
Name:	Teresa D. Ross
Title:	USMC Privacy Act/FOIA Officer
Organization:	HQMC ARSF
Work Telephone Number:	(703) 614-4008
DSN:	
Email Address:	SMBHQMCPRIVACYACT@USMC.MIL
Date of Review:	

Component CIO Signature (Reviewing Official)	CAREY.ROBERT.JOSEPH.1035258368 Digitally signed by CAREY.ROBERT.JOSEPH.1035258368 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=CAREY.ROBERT.JOSEPH.1035258368 Date: 2010.01.21 17:13:22 -05'00'
Name:	Robert J. Carey
Title:	Department of the Navy Chief Information Officer
Organization:	Department of Navy
Work Telephone Number:	(703) 602-1800
DSN:	
Email Address:	robert.carey@navy.mil
Date of Review:	

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.