



UNITED STATES MARINE CORPS  
MARINE CORPS AIR STATION YUMA  
BOX 99100  
YUMA, ARIZONA 85369-9100

StaO 5211.1  
OJAD  
3 Dec 09

STATION ORDER 5211.1

From: Commanding Officer  
To: Distribution List

Subj: PRIVACY ACT

Ref: (a) 5 U.S.C. 552a  
(b) DoD Directive 5400.11  
(c) SECNAVINST 5211.5E

Encl: (1) Rules of Access

1. Situation. Per the references, the Privacy Act (PA) was established to give greater control over the way records about an individual are filed, maintained, protected, retrieved and to eliminate needless intrusions of personal privacy through the maintenance of records.

2. Mission. Implement procedures pursuant to the references that govern the collection, safeguarding, maintenance, use, access, amendment, disposal, and dissemination of personal information in PA Systems of Records (SOR) kept by Marine Corps Air Station (MCAS) Yuma, departments and tenant units.

3. Execution

a. Commander's Intent and Concept of Operations.

(1) Commander's Intent

(a) It is the policy of this command that all personnel comply fully with the purpose and requirements of the references. Specifically, only such personal information as is relevant and necessary to accomplish a purpose or mission as required by statute or executive order will be kept on an individual. Additionally, consideration must be given to the length of time such information is needed and disposition instructions must be provided for any records collected and maintained which contain any Protected Personal Information (PPI). Proper disposal of such records should prevent identification of specific records.

(b) Definitions

1. Protected Personal Information (PPI). Any information or characteristic(s), specific to an individual, that may be used to distinguish or trace an individual's identity, such as their name, social security number (SSN), or biometric records.

2. System of Records (SOR). A group of records under the control of a Department of Navy (DON) activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual.

(2) Concept of Operations. To ensure knowledge of the references throughout MCAS Yuma; to ensure that all MCAS Yuma military members and civilian/contractor employees are made fully aware of their rights and responsibilities under the provisions of the PA and to ensure privacy management practices and procedures in place.

b. Subordinate Element Missions

(1) Judge Advocate Department

(a) PA Coordinator. The Commanding Officer, MCAS Yuma designates the Civil Law Attorney or alternatively, the Legal Assistance Attorney as the PA Coordinator for MCAS Yuma. The PA Coordinator will be located at the Joint Law Center. The duties of the PA Coordinator are as follows:

1. Serve as the primary point of contact for administration of the PA program;

2. Provide training on an as needed basis;

3. Review requests for non-routine personal data and provide a recommendation stating whether or not the disclosure is in conflict with the PA;

4. Inform the Commandant of the Marine Corps (ARSF) of the need to establish, amend, or delete a new Marine Corps PA System of Record Notice (SORN);

5. Ensure that no official files are maintained on individuals that are retrieved by a personal identifier

unless SORN exists allowing such collection;

6. Maintain liaison and work closely with installation PA system managers and local record managers;

7. Conduct staff assistance visits and/or program evaluations within MCAS Yuma;

8. Process PA complaints;

9. Conduct annual reviews of SORN;

10. Ensure no personally protected information is placed on public websites or in public folders.

(2) MCAS Yuma Departments and Tenant Units

(a) PA Representative. Every department and unit within MCAS Yuma will appoint a PA Representative. The duties of the PA Representative are as follows:

1. Serve as the primary point of contact for administration of the privacy program within their department or unit;

2. Maintain direct liaison with the MCAS Yuma PA Coordinator on all PA issues;

3. Maintain an accurate list of records maintained within their department or unit;

4. Maintain an accurate list of all local records managers within their department or unit;

5. Ensure annual training is provided to all records managers within their department or unit;

(3) System Managers and Local Record Managers. System managers and local record managers (sometimes referred to as custodians) are indicated in published SORN located at the Department of the Navy's PA website:  
<http://www.privacy.navy.mil>.

(a) Duties of the system managers and local record managers are:

1. Oversee the collection, maintenance, use, and dissemination of information from a PA SOR;
2. Ensure that all personnel authorized access to the system or engaged in the development of procedures for handling records are informed of the requirements of the PA and the protection of protected personal information;
3. Determine the content and procedures for operating the system;
4. Ensure that no unpublished system of records on individuals is maintained, and that no new or significantly changed system exists without the required pre-publication in the Federal Register.
5. Provide the unit PA representative an accurate list of records maintained within their respective area;
6. Respond to requests from individuals for information in the system. Requests for non-routine personal data shall be referred to the MCAS Yuma PA Coordinator;
7. Maintain direct liaison with the MCAS Yuma PA Coordinator and the department or unit PA Representative;
8. Maintain an accurate disclosure of accounting;
9. Complete annual training consisting of Roles and Responsibilities of PA SOR managers slide presentation as provided by the MCAS Yuma PA Coordinator.

c. Coordinating Instructions

(1) Training. MCAS Yuma PA SOR Managers are responsible for ensuring all personnel whose duties involve the collection, safeguarding, maintenance, use, access, amendment, disposal, and dissemination of personal information in a PA SOR are educated and trained in accordance with the provisions of reference (c). MCAS Yuma PA SOR managers will complete the Roles and Responsibilities of PA SOR Managers training annually. The Roles and Responsibilities Training is available through the MCAS Yuma PA Coordinator. Additional training tools are

available through the Department of the Navy (DON) website at [www.privacy.navy.mil](http://www.privacy.navy.mil).

(2) Access and Notification Procedures

(a) Enclosure (1) states the rules of access which a system manager or local record manager should furnish to an individual requesting access to his/her record(s).

(b) It is generally advisable to require an individual to make a request in writing; however, a service member requesting to view his/her own service record book should normally not be required to submit a request in writing. All other requests for access shall be acknowledged within 10 working days and reviewed by the PA Coordinator.

(c) The request cannot be considered if:

1. The identity of the requester is not verified;

2. The requester did not furnish adequate information to locate a record within a system; or,

3. The request was forwarded to an official not having custody or responsibility for the SOR concerned.

(d) The local record manager or system manager will inform the individual of the additional information needed or the correct way of requesting access.

(e) The local record manager or system manager will not deny access to an individual who is the subject of the record solely for refusing to divulge his/her social security number (SSN), unless it is the only means of retrieving the record or verifying an individual's identify.

(3) Amendment of Records. Individuals have a right to request that their records be amended by correction, deletion or other changes. Amendments under the PA are limited to factual matters. Judgmental decisions shall be challenged via the Board for Correction of Naval Records.

(4) Collection of Personal Information. Whenever possible, collect information for SOR directly from the individual to whom the record pertains. Before requesting an

individual to provide his/her SSN the individual must be advised, by means of a Privacy Act Statement (PAS), whether providing the SSN is mandatory or voluntary, by what law or other authority the SSN is solicited, and what uses will be made of the SSN.

(5) Disclosure

(a) Besides disclosure of records to the individual to whom the record pertains, disclosure may not be made of any record to a third party, in the absence of a written consent, unless disclosure of the record is authorized under one or more of the conditions cited as follows: "Need to know" Department of Defense (DoD) personnel, Freedom of Information Act (FOIA), routine use, Bureau of the Census, statistical research or reporting, national archives, civil or criminal law enforcement activity, emergency conditions, comptroller general, order of a court, and members of Congress.

(b) OPNAV 5211/9 Accounting Disclosure Form

1. System managers and local record managers shall keep an accurate accounting of the name and address of the person or agency that the disclosure is made, date, nature and purpose of disclosure. Disclosures made to members of the agency, who have a need for the record in the performance of their duties, as well as information required to be disclosed under the FOIA, need not be listed on the accounting disclosure form. OPNAV 5211/10, the accounting disclosure form, can be found at [www.privacy.navy.mil](http://www.privacy.navy.mil).

2. Retain the disclosure accounting form for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.

3. Upon request from the individual of the record, system managers or local record managers must make available all disclosure accounting information with the exception of a disclosure made to another agency or an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired.

4. Inform any person or other agency about any correction to the record that has been disclosed.

(6) Criminal Penalties. Knowingly and willfully obtaining records under false pretenses, disclosing privacy data to any person not entitled to access, and/or maintaining unauthorized records can result in a misdemeanor criminal charge and a fine of up to \$5000.

(7) Denial Authority. The Commanding Officer, MCAS Yuma is the Denial Authority for all SOR maintained by MCAS Yuma.

4. Administration and Logistics. Distribution statement "B" directives issued by this command are published electronically and can be accessed online via the MCAS Yuma homepage at <https://intranet.mciwest.usmc.mil/yuma/default.aspx>.

5. Command and Signal

a. Command. This order is applicable to all MCAS Yuma departments and tenant units.

b. Signal. This order is effective the date signed.

  
M. A. WERTH

DISTRIBUTION: B

Rules of Access

1. Requests for access must be submitted in writing to the system manager or local record manager identified in the governing Privacy Act system of record notice, as published in the Federal Register, and must contain the criteria set out in the records access section of the Privacy Act system of record notice, to include a written signature.
2. An individual desiring to review records pertaining to himself is urged to submit his request 10 days prior to the desired review date. Every effort will be made to provide access more rapidly when necessary. However, records ordinarily cannot be made available for review on the day of the request. When the request is to provide the individual's records directly to an authorized representative, other than the parent of a minor or legal guardian, a signed authorization is required, specifying the records to be released.
3. Requests must contain the specific identifying information set out in the governing Privacy Act system of record notice, e.g., full name, social security number, etc.
4. Indicate when and where the record may be reviewed.
5. When a request is made in person, the custodian will require presentation of identification before providing an individual access to records pertaining to that individual. Acceptable forms of identification are a military identification card, CAC identification, base or building pass, driver's license, medical card, or similar picture identification.
6. When a request is made by mail or other written form, verification of identity may be obtained by requiring the individual to provide certain minimum identifying data, such as date of birth and some items of information in the record that only the concerned individual would likely know.
7. Individuals may be accompanied by a person of their own choosing when reviewing the records. However, the custodian will not discuss the record in the presence of the third person without the written authorization of the individual to whom the records pertain. The following conditions also apply:
  - a. Do not deny access to an individual who is the subject of a record solely for refusing to divulge their social security

3 Dec 09

number, unless it is the only means of retrieving the record or verifying identity.

b. Do not require the individual to explain why the record is being sought under the Privacy Act.

8. When requested, copies of the record will be provided and the response may be made by mail. The system or records manager must ensure, however, that such disclosure does not release the social security number of others that may be contained within the subject matter's record.

9. A medical record will not be released to the individual if in the judgment of the physician the information contained therein could have an adverse effect on the individual's physical or mental well-being. In this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician.

10. Questions concerning these rules of access or information contained in the record should be addressed to that record's system manager set out in the governing Privacy Act system of record notices, as published in the Federal Register.