



UNITED STATES MARINE CORPS

MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904-5001

ASO 5211.1
ADJ
10 NOV 2009

AIR STATION ORDER 5211.1

From: Commanding Officer
To: Distribution List

Subj: PRIVACY ACT

Ref: (a) 5 U.S.C. § 552a (Privacy Act of 1974)
(b) MCEN IA Dir of 9 Apr 09
(c) SECNAVINST 5211.5E
(d) SECNAVINST 5720.42F
(e) MCIEASTO 5211.1A
(f) SECNAVINST M-5210.1
(g) MCIEASTO 3040.1C

Encl: (1) MCASBFT/ADJ/5211/1 (Privacy Act and Routine Use Request Form)
(2) Disclosure Accounting Form (OPNAV 5211/9)
(3) General Purpose Privacy Act Statement (OPNAV 5211/12)
(4) MCASBFT/ADJ/5211/2 (Record of Disclosure/Consent Authorization Form)

1. Situation. To publish the policies and procedures governing the collection, safeguarding, maintenance, public notice, use, access, amendment and dissemination of personal information contained in a systems of records maintained at Marine Corps Air Station (MCAS) Beaufort.

2. Mission. Reference (a) establishes the right to individual privacy as one protected by the United States Constitution. It also provides for safeguarding that privacy in the compilation and use of records pertaining to individuals and grants them access to those records which pertain to them personally.

3. Execution

a. Commander's Intent and Concept of Operations. Subject to directives of higher authority, it is the policy of this Command that all personnel comply with the purposes and requirements of references (a) through (e). In furtherance of this policy, only such information as is reasonably necessary to accomplish a purpose or mission required by higher authority will be kept on any individual. Additional consideration must be given to the length of time such information is needed. Disposition instructions must be provided for any records collected and maintained which contain any Personally Identifiable Information (PII). Reference (f) provides appropriate instructions for retention and disposal of records.

b. Subordinate Element Missions

(1) Privacy Act Officer. The Privacy Act (PA) Officer is the Station Adjutant. The PA Officer will be appointed in writing and serves as the principle point of contact/responsible officer on all PA matters. The PA Officer shall:

(a) Appoint in writing an Assistant PA Officer and Coordinator for the air station.

(b) Oversee the administration of the Command's PA program; reviews and resolves PA complaints; develops a privacy education, training and awareness program, revises and validates the Privacy Impact Assessment (PIA) for the command's information systems. Conduct staff assistance visits/program evaluations within the command to review compliance with the references.

(c) Conduct and document privacy awareness training for all personnel aboard MCAS Beaufort to include military, civilian, contractor, volunteers, non-appropriated fund employees, etc. Training options include: "All Hands" awareness briefing; memorandum to staff; formal training; circulation of privacy act briefing. Additional training tools are available at <http://privacy.navy.mil/training>.

(d) Notify command personnel of this policy and address steps necessary to ensure that PII is not compromised.

(e) Establish a Privacy Team to identify ways to preclude inadvertent release of PII.

(f) Ensure that Assistant PA Officer and PA Coordinator are familiar with all directives pertaining to their assignments.

(g) Ensure that the Commanding Officer, MCAS Beaufort is briefed on any PA breaches and that those breached are reporting in accordance with reference (e).

(2) Assistant Privacy Act Officer/Coordinator. The Assistant PA Officer/Coordinator will be appointed in writing. The Assistant PA Officer is the Station Adjutant Chief. The PA Coordinator is Ms. Stephanie L. Snow, MCAS Adjutant's Office. The Assistant PA Officer/Coordinator shall:

(a) Become familiar with all orders and regulations pertaining to their assignment.

(b) Work closely with the PA Officer and Department/Section Heads to conduct training, evaluate what PII can be removed from routine message traffic, review web site postings, review command electronic bulleting boards, etc., to ensure appropriate processes are in place to minimize the misuse and overuse of PII information that could be used to commit identity theft. The Assistant PA Officer/Coordinator should also ensure that their PA systems of records managers have a copy of the appropriate PA systems notice and understand PA rules.

(c) Assist Department Head/Section Heads in examining their business practices to eliminate the unnecessary collection, transmittal and storage of PII.

(d) Provide training to DON military members/employees who maintain PII on their laptop computers/blackberry, who telecommute, work from home, or take work home, etc., to ensure information is properly safeguarded against loss/comprise. Should a loss occur, ensure they are aware of the procedures for reporting the loss.

(e) Review internal directives, forms, websites, share portals, practices, and procedures, including those having PA statements (PAS) or documents where PII is solicited.

(f) Maintain liaison with records management officials to ensure that documents that contain PII are retained only when necessary and disposed of properly in accordance with reference (f).

(g) Advise Headquarters, U.S. Marine Corps (HQMC) promptly of the need to establish a new PA system of records; amend or alter an existing record; or delete a system of record that is no longer needed.

(h) Compile and maintain a listing of all systems of records to ensure no unauthorized collection occurs. Review this listing annually as required by reference (c), paragraph 7(h)(16). This listing will include the name of the system, system notice number, system manager, review date and collection date.

(i) Process all PA requests for information under MCAS Beaufort purview according to reference (c), maintain a complete administrative record to include a tracking database, response letters, referrals, releases and records according to the retention schedule in reference (e). Refer documents to the Freedom of Information Act (FOIA) Officer for release determination if documents are determined questionable.

(3) Commanding Officer, Headquarters and Headquarters Squadron/Department and Section Heads/PA Systems Managers

(a) Designate, in writing, a PA systems manager for each department/section.

(b) Ensure proper procedures are established to safeguard PII that is contained in any systems of records. PII is any information that contains privacy sensitive data (e.g., home address, date of birth, Social Security Number (SSN), credit card or charge card account numbers, etc.) and is pertaining to a service member, civilian employee (appropriated and non-appropriated fund), military retiree, family member, or another individual affiliated with this Command (i.e., volunteers). PII must be protected from unauthorized disclosures.

(c) Examine business practices to eliminate the unnecessary collection, transmittal and posting of PII in directives, forms, websites, share portals, and databases.

(d) Evaluate risks for potential compromise of PII held in activity files, databases, etc., to ensure proper safeguards are in place to prevent unauthorized disclosures. Revise protocols as necessary.

(e) Ensure that PA systems of records are properly safeguarded and that PII contained in the systems of records are properly disposed of, when no longer required, in accordance with reference (f).

(f) Ensure no official files are maintained on individuals that are retrieved by name or other personal identifier without first ensuring a system of records notice exists that permits such collections.

(g) Provide a listing of all systems of records to ensure no unauthorized collection occurs. Review this listing annually as required by reference (c), paragraph 7(h)(16). This listing will include the name of the system, system notice number, system manager, review date and collection date.

(h) Ensure that all personnel assigned to the squadron/department/section complete privacy act refresher training annually and that new joins check-in with the Station PA Coordinator located in Building 601, Room 123 for the New Join Privacy Act Brief.

(4) System Users Responsibility. Per reference (c) all DON employees/contractors are responsible for safeguarding the privacy of individuals and confidentiality of PII. A Systems User is any person aboard MCAS Beaufort that collects, transmit, or process documents and/or systems that contain PII. PII includes personal information about an individual that identifies, relates, or is unique to, or describes him or her (e.g., SSN, age, marital status, race, salary, home/cell phone numbers, etc.). All system users are responsible for the administration and supervision of the PA within their area of responsibility in accordance with published instructions from higher authority. Additionally, system users shall:

(a) Ensure that PII contained in a system of records, to which they have access or are using to conduct official business, is protected so that the security and confidentiality of the information is preserved.

(b) Not disclose any information contained in a system of records by any means of communication to any person or agency, except as authorized by this Order or the specific PA systems of records notice.

(c) Not maintain unpublished official files that would fall under the provisions of reference (a).

(d) Safeguard the privacy of individuals and confidentiality of PII contained in a system of records.

(e) Properly mark all documents containing PII data (e.g., letters, e-mails, message traffic, etc.) as "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE - Any misuse or unauthorized disclosure can result in both civil and criminal penalties."

(f) Not maintain privacy sensitive information in public folders.

(g) Remove PII from documents prior to posting or circulating information to individuals without an "official need to know."

(h) Report any unauthorized disclosure of PII from a system of records to the Station PA Officer via the chain-of-command.

(5) Training

(a) All supervisors shall be responsible for ensuring that all personnel, whose duties are responsible for designing, developing, maintaining, custody and use of systems of records affected by the PA are educated and trained in the provisions of the references and this Order.

(b) References (b) and (c) provide the DON training programs. Training will be conducted upon joining this command and will be conducted annually.

(6) Breach Reporting

(a) A breach is an actual or possible loss of control, unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. All personnel will report any known or suspected breaches to the PA Officer via the chain-of-command.

(b) The PA Officer will report known or suspected breaches in accordance with the guidance set forth in reference (b) and (e).

(7) PA Enforcement Actions

(a) Administrative Remedies. Any individual who alleges they have been adversely affected by a violation of reference (a) at this command may seek relief from the Secretary of the Navy through administrative channels. It is recommended that the individual first address the issue through the PA Officer/Coordinator or a systems manager that have cognizance over the relevant records or supervisor (if a government employee). If the complaint is not adequately addressed, the individual may contact the Chief of Naval Operations (CNO) (DNS-36) or the Commandant of the Marine Corps (ARSF) for assistance.

(b) Civil Court Actions. After exhausting administrative remedies, an individual may file a civil suit in federal court against a DON activity for the following acts:

1. Denial of an Amendment Request. The activity head or his/her designee wrongfully refusing the individual's request for review of the initial denial of an amendment or after review, wrongfully refusing to amend the record.

2. Denial of Access. The activity wrongfully refuses to allow the individual to review the record or wrongfully denies his/her request for a copy of the record.

3. Failure to Meet Recordkeeping Standards. The activity fails to maintain an individual's records with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination about the individual's rights, benefits, or privileges and, in fact, makes an adverse determination based on the record.

4. Failure to Comply with PA. The activity fails to comply with provisions, rules and regulations set forth under references (a) through (c), and that action thereby causes the individual to be adversely affected.

(c) Civil Remedies. In addition to specific remedial actions, reference (c) provides for the payment of damages, court costs, and attorney fees in some cases.

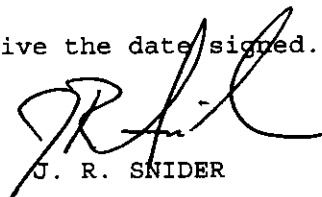
(d) Criminal and Other Penalties. Reference (c) authorizes criminal penalties against individuals for violations of its provisions, each punishable by fines up to \$5,000. Appropriate corrective action or disciplinary action for a breach of PII is at the discretion of MCAS Beaufort Commanding Officer or Headquarters and Headquarters Squadron, Commanding Officer, respectively on a case-by-case basis. Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. The minimum consequence that the command will consider is prompt removal of authority to access information or systems from individuals who demonstrate egregious disregard or a pattern of error in safeguarding personally identifiable information.

4. Administration and Logistics. Recommendations concerning the contents of this Order may be forwarded to PA Officer via the appropriate chain of command.

5. Command and Signal

a. Command. This Order is applicable to all military personnel, DON civilians, and contractors assigned to MCAS Beaufort including all air station activities.

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



J. R. SNIDER

DISTRIBUTION: A

PRIVACY ACT AND ROUTINE USE REQUEST FORM

PRIVACY ACT STATEMENT

Under the AUTHORITY 5 U.S.C. 552(a) and E.O. 9397 (SSN), this form is FOR OFFICIAL USE ONLY for the PURPOSE to track, process, and coordinate individual requests for access and amendment of personal records; to process appeals on denials of requests for access or amendment to personal records; to compile information for reports, and to ensure timely response to requesters. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside DoD as a ROUTINE USE pursuant to 5 U.S.C. 552a(b)(3). DISCLOSURE is MANDATORY.

Commanding Officer
MCAS
Attn: Adjutant (Privacy Act Coordinator)
PSC Box 55001
Beaufort, SC 29904-5001
Date _____

Name _____ Rank _____
Address _____
City _____ State _____ Zip Code _____
E-MAIL: _____
SSN _____ Incident Number _____

I _____, am requesting under Privacy Act of 1974, all information and records on my incident(s) dated _____. Furthermore, I declare under penalty of perjury under the laws of the United States of America that all information provided is true and accurate to the best of my knowledge.

Type of Request (Select Only One)

- PRIVACY ACT (PA)**
(Personal information directly about the individual, SRB, OPM)
- ROUTINE USE**
(OFFICIAL USE, Federal, State and local agency for civil or criminal or for hiring, retention, insurance company, accident reports, security clearance and contract)

Listed below is a detail description of what I am requesting:

Do you want to pick up the report or have it mailed to you? PICK UP MAILED

Signature _____
Home Number _____
Work Number _____
Cell Number (optional) _____

FOR OFFICIAL USE ONLY (FOUO)-PRIVACY ACT SENSITIVE
You may return this request in person to the Station Adjutant's Office, mail, e-mail at BERT_MCASPrivacyActRequest@usmc.mil, or fax at (843) 228-7032. For additional information, call Ms. Snow at (843) 228-7921.

DISCLOSURE ACCOUNTING FORM

RECORD OF DISCLOSURE

UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM THIS RECORD COULD SUBJECT THE DISCLOSURE TO CRIMINAL PENALTIES

- 1. This is to remain a permanent part of the record described below.
- 2. An entry must be made each time the record or any information from the record is viewed by, or furnished to any person or agency, except:
 - a. Disclosure to DOD or DON personnel having a need to know in the performance of their official duties.
 - b. Disclosure of items listed in paragraphs 13b(2)(e) and (f) of SECNAVINST 5211.5 series.

TITLE & DESCRIPTION OF RECORD

DATE OF DISCLOSURE	METHOD OF DISCLOSURE	PURPOSE OF AUTHORITY	NAME & ADDRESS OF PERSON OR AGENCY TO WHOM DISCLOSED, WITH SIGNATURE IF MADE IN PERSON

DATE OF DISCLOSURE	METHOD OF DISCLOSURE	PURPOSE OF AUTHORITY	NAME & ADDRESS OF PERSON OR AGENCY TO WHOM DISCLOSED, WITH SIGNATURE IF MADE IN PERSON

GENERAL PURPOSE PRIVACY ACT STATEMENT	
PART A - IDENTIFICATION OF REQUIREMENT	
1. REQUIRING DOCUMENT (Describe - SECNAVINST, OPNAVNOTE, SECNAV ltr, etc.)	2. SPONSOR CODE
3. DESCRIPTIVE TITLE OR REQUIREMENT (Form title, report title, etc.)	
PART B - INFORMATION TO BE FURNISHED TO INDIVIDUAL	
1. AUTHORITY	
2. PRINCIPLE PURPOSE(S)	
3. ROUTINE USE(S)	
4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION	
PART C - IDENTIFICATION OF FORM/REPORT/OTHER REQUIREMENT	
1. FORM NO./REPORT CONTROL SYMBOL/ OTHER IDENTIFICATION	PRIVACY ACT STATEMENT

OPNAV 5211/12 (MAR 1992)

RECORD OF DISCLOSURE/CONSENT AUTHORIZATION FORM

PRIVACY ACT STATEMENT

Under the AUTHORITY 18 U.S.C. 5013 and E.O. 9397, this form is for official use only. The PURPOSE of this form is to track, process, and coordinate individual requests for access and amendment of personal records; to process appeals on denials of requests for access or amendment to personal records; to compile information for reports, and to ensure timely response to requesters. A record from a system or records maintained by the DoD component may be disclosed as a ROUTINE USE to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component for a decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, the reporting of an investigation of an employee, or the issuance of a license, grant, or other benefit. DISCLOSURE IS MANDATORY.

1. IDENTIFYING INFORMATION ON SUBJECT

a. Name of Individual: _____

b. Grade/Rank: (Enter if not USMC) _____

c. Title: _____

d. Individual's Social Security Number (999999999): _____

2. PERTINENT DATA TO WHOM DISCLOSURE WAS MADE

a. Date of Disclosure (DD MMM YYYY): _____

b. Nature and Purpose of Disclosure: _____

c. Name of Person to Whom Disclosure Made: _____

d. Address: _____

Phone Number: _____

e. Office to Which Disclosure was Made: _____

3. INFORMATION ON PERSON MAKING DISCLOSURE

a. Name of Individual: _____

b. Grade/Rank: (Enter if not USMC) _____

c. Office or Title: _____

d. Duty Station Address: _____

I HEREBY AUTHORIZE THE MARINE CORPS TO VERIFY MY SOCIAL SECURITY NUMBER AND TO DISCLOSE MY INFORMATION FOR OFFICIAL USE ONLY.

Signature of Individual: _____

Date (DD MMM YYYY): _____

Print Form

Reset Form