



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEAST-MCB CAMLEJO 5211.6
G-1
25 SEP 2012

MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE ORDER 5211.6

From: Commanding General
To: Distribution List

Subj: PRIVACY ACT (PA)

Ref: (a) 5 U.S.C. § 552a (Privacy Act of 1974, as amended)
(b) SECNAVINST 5211.5E
(c) SECNAVINST 5720.42F
(d) SECNAV M-5210.1
(e) MCIEASTO 5720.1A
(f) MCIEASTO 5211.5

Encl: (1) Training Roster (MCIEAST-MCB CAMLEJ/G-1/ADJ/17)
(2) PA Self Assessment Form (MCIEAST-MCB CAMLEJ G-1/ADJ/5211.6/25)
(3) MCIEAST-MCB CAMLEJ Privacy Act and Routine Use Request Form
(MCIEAST-MCB CAMLEJ/G-1/ADJ/5211.1/3)
(4) Disclosure Accounting Form (OPNAV 5211-9)

1. Situation. Pursuant to references (a) through (f), this Order provides policy and procedural guidance to ensure individuals are aware of their rights and responsibilities under the provisions of the Privacy Act (PA) of 1974, and to implement privacy management practices that balance the need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy.

2. Cancellation. MCIEASTO 5211.1B and BO 5211.6D.

3. Mission. To promulgate policies and procedures governing the collection, safeguarding, maintenance, public notice, use, access, amendment, and dissemination of personal information contained in a system of records maintained by Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ).

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Reference (a) establishes the right to individual privacy, provides for safeguarding privacy in the compilation and use of an individual's records, and grants them access to those records which contain their personal information.

(2) Concept of Operations. All personnel within MCIEAST-MCB CAMLEJ and tenant commands shall fully comply with the requirements of references (a) through (f) in order to safeguard personal information resident in systems of records. Only information reasonably necessary to accomplish a purpose or mission required by higher authority will be kept on any individual. Additionally, consideration must be given to the length of time such information is required. Reference (d) provides appropriate instructions for retention and disposal of records.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

b. Subordinate Element Missions

(1) MCIEAST-MCB CAMLEJ Assistant Chief of Staff (AC/S), G-1. The Commanding General (CG), MCIEAST-MCB CAMLEJ, has designated in writing the AC/S G-1 as the Command PA Coordinator for MCIEAST-MCB CAMLEJ. The Command PA Coordinator falls under the cognizance of the Adjutant and shall:

(a) Be designated and appointed in writing as the Command PA Coordinator for MCIEAST-MCB CAMLEJ.

(b) Serve as the principal point of contact on PA matters.

(c) Appoint in writing a Command PA Program Officer and Coordinator to administer the program.

(2) Command PA Program Coordinator shall:

(a) Work closely with departmental PA/System of Records Managers to ensure appropriate processes are in place to minimize the misuse of personal data.

(b) Advise Headquarters, U.S. Marine Corps (HQMC) when a need to establish a new PA system of records, amend or alter an existing system of records, or delete a system of records that is no longer required.

(c) Work closely with command officials to conduct annual PA training as well as system of records notice (SORN) training.

(d) Issue implementing guidance regarding the Command's PA program.

(e) Compile and maintain a listing of all systems of records for MCIEAST-MCB CAMLEJ, to ensure no unauthorized collection occurs. This list should be reviewed annually as required by reference (b).

(f) Ensure all PA system of records Managers have a copy of the appropriate PA SORN and understand PA rules.

(g) Publish an annual bulletin identifying the SORN maintained by MCIEAST-MCB CAMLEJ.

(h) Perform unannounced self-assessments visits to identify strengths and weaknesses and to determine training needs of personnel who work with systems of records. Supervisors will conduct self-assessments on their area of responsibility (AOR).

(i) Ensure official files retrieved by name or other identifier are not maintained on individuals without first ensuring a SORN exists that permits such collection.

(j) Maintain liaison with records management officials regarding the maintenance and disposal procedures and standards as appropriate, per reference (b).

2 5 SEP 2012

(3) MCIEAST-MCB CAMLEJ Subordinate Commanders and Department PA/System of Records Managers shall:

(a) Be appointed in writing.

(b) Ensure annual PA training is conducted and documented as directed by the Command PA Program Coordinator. Provide training statistical information to the Command PA Program Coordinator. Utilize enclosure (1) to track group PA training sessions. Training certificates and rosters are to be maintained at the departmental level for two years.

(c) Ensure all personnel authorized access to the system of records, or engaged in the development of procedures for handling records, are informed of the requirements of the PA with regards to information.

(d) Ensure compliance with including PA Statements (PAS) on forms, per reference (b).

(e) Mark all documents that contain personal data "For Official Use Only", consider using a header/footer that reads: "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

(f) Ensure no unpublished system of records on individuals is maintained, and no new or significantly changed system exists. Current authorized and published systems can be located on the Department of the Navy Chief Information Officer (DONCIO) website: <http://www.doncio.navy.mil>.

(g) Ensure that only those Department of Defense (DoD)/Department of the Navy (DON) officials with a "need to know" in the official performance of their duties have access to information contained in a system of records.

(h) Ensure records are kept in accordance with retention and disposal requirements set forth in reference (c).

(i) Report any suspected loss or compromise of personal data from a system of records to the Command PA Program Manager.

(j) The department system of records Manager will determine the relevancy and necessity of information during the development of a new system of records or when an amendment to an existing system is proposed.

(k) Conduct annual self-assessments visits to ensure compliance with the PA program utilizing enclosure (2).

c. Coordinating Instructions

(1) Training

(a) All personnel whose duties include: designing, developing, and maintaining custody and use of a system of records affected by the PA shall be educated and trained in the provisions of references (a) through (f), and this Order.

25 SEP 2012

(b) Reference (b) provides information on DON training programs and resources. Training materials and links are located on the MCIEAST-MCB CAMLEJ external site:
<http://www.mcieast.marines.mil/StaffOffices/Adjutant/PrivacyActProgram.aspx>

(c) Under reference (b), all individuals who work with a PA system of records shall receive SORN training annually. Advise and stress to individuals their rights and responsibilities per the SORN for each system utilized.

(2) Federal Register of System of Records. In line with one of the basic principles of the PA, there are no records maintained which are kept secret. The Act requires that federal agencies make public the existence and character of personal data systems through annual publication of SORNs in the Federal Register located at <http://www.federalregister.gov>. To establish, amend, modify and delete SORNs, contact Chief of Naval Operations (CNO) (DNS-36)/CMC (ARSF), per the guidance provided in reference (b).

(3) Collection of Information and Maintenance of Records/Use of Forms

(a) Reference (a) requires organizations that gather information from individuals that is contained in a system of records, to provide individuals with sufficient guidance to ensure they can make an informed decision about providing the requested information. Reasonable effort must be made to ensure personal data maintained is accurate, relevant, timely, and as complete as necessary to ensure fairness in any determination made on the basis of the record. The PA authorizes civil action against an agency for failure to maintain records accordingly.

(b) The PA requires that any form, questionnaire, report, or other media used to collect data from employees must be accompanied by a PAS. This PAS advises the individual as to the authority for requesting the data, the principal purpose for which it is requested, the routine uses made of the data, whether or not it is mandatory or voluntary, and what, if any, consequences may result from failing to provide the information.

(c) References (a) and (b) provide additional guidance relative to the use of PAS when requesting personal information.

(4) Recording of Statements Made in Person. Except when authorized by statute or regulation or other lawful authority, manual verbatim transcriptions or the use of electronic or mechanical recording devices in hearings, meetings, interviews, and conversations are authorized only when advance notification is given to all participants that the recording or transcription will occur. Investigative personnel should take note of this paragraph.

(5) Special Instructions for Use and Safeguarding of Information in the Automated System. Per reference (b), all PA information that is obtained, copied, electronically stored, and/or printed from an electronic system will be properly marked, safeguarded, and destroyed. Ensure that only those who have an official need to know in their official capacity have access to the collected information. Detailed safeguards and exemption release information are provided on each SORN.

25 SEP 2012

(6) PA Self Assessments. This serves to identify strengths and weaknesses, determine training needs of personnel, and to identify deficiencies, irregularities, and significant problems. Document remedial actions taken to correct problems identified. Utilize the self-assessment form at enclosure (2) to measure compliance with the PA program. Privacy Act Managers will retain self-assessment reports in accordance with the disposition schedule of two years or until the next self-assessment is completed, per references (b) and (d).

(7) Breach Reporting

(a) Reports. Breach reports are required following evidence of an actual or possible loss of control, unauthorized access of personal information, or 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. Reporting of PA Breaches will follow the guidance set forth in reference (b).

(b) Action. The process outlined will be used for reporting a known or suspected loss of PA information from a system of record. The designated official of the accountable command/activity will contact the MCIEAST-MCB CAMLEJ Command PA Program Officer or Coordinator by telephone. Per reference (b), within one hour of the discovery, the department/command PA coordinator shall complete and send the Initial Breach Report to the Command PA Program Coordinator for submission to HQMC. Within 24 hours, provide an after action report to include lessons learned, per reference (b).

(8) Access to Records

(a) References (a) and (b) provide that individuals must be allowed access to records about themselves, except where specific exemption has been approved by the Secretary of the Navy (SECNAV). Persons seeking access to records about themselves may inspect the record, copy it, or be furnished a copy and may request correction of the record when an error is found. In addition, they may designate another person to accompany them to review their record in the accompanying person's presence. Extreme care must be taken not to inadvertently disclose another individual's record.

(b) Information in the Marine Corps Total Force System is periodically audited and requires the presence of the individual to ensure accuracy.

(c) All other requests for notification, access, or amendments to records held by each command should be in writing to each respective PA Officer. Personnel assigned to MCIEAST-MCB CAMLEJ will send their request to the PA Release Officer located in building 1, room 236. Requests for access will be acknowledged within ten working days, and access provided within 30 days. Enclosure (3) may be used for requesting information.

(d) Amendment of Records. Individuals have a right to request amendment to their record if they believe the information to be in error. Amendments are limited to correcting factual or historical matters (dates and locations of service, participation in certain actions or activities)--not matters of opinion -- except when based solely on inaccurate facts and those facts have been thoroughly discredited. Amendment requests must be made in writing with proper documentation provided showing the record to be in error.

The burden of proof rests with the individual. The system of records manager does not have to agree, but should amendment of the record be denied, the decision is appealable. Further information on appeal processes are provided in reference (a).

(9) Freedom of Information Act (FOIA) and PA Release Office

(a) FOIA Office. To protect the personal privacy of other individuals within a PA record, the document shall be referred to the FOIA Office located in building 1, room 236 for redaction. The individual will be notified in writing if a record is referred to the FOIA office for release determination.

(b) PA Release Office. Process all PA requests for information according to reference (b), maintain a complete administrative record to include a tracking database, response letters, referrals, releases, and records according to the retention schedule in reference (c). Refer documents to the FOIA Officer for release determination if documents are determined questionable, as outlined in reference (f).

(c) Disclosure. A first party access request will be submitted to the command's PA Officer for collection and release using enclosure (3). Documents containing information pertaining to the requester and other parties will be referred, pursuant to references (c) and (f), to the FOIA for release determination. If personal information is determined to be exempt from disclosure, written documentation from each individual who has personal information in the file must authorize release (enclosure (3) may be utilized). Responses to inquiries from sources outside the Department of Defense (DoD) about MCIEAST-MCB CAMLEJ personnel will be forwarded for release by the Commanding General, MCIEAST-MCB CAMLEJ (Attn: G-1 PA Coordinator).

(10) Disclosure Accounting

(a) An accurate accounting must be kept on all disclosures made from a record (including those made with the consent of the individual), except those made to DoD personnel for use in performing their official duties and those disclosures made under FOIA. Personnel acting in their official capacity will present an authorization letter signed by a command official, specifying the records sought, to the system of records Manager in order to receive a copy of the official record.

(b) Disclosure accounting records are not required when an individual seeks a record about themselves when a record may be produced immediately by the system of records manager.

(c) Enclosure (4) is an example of the disclosure accounting form. Each system of records Manager will keep an accurate accounting of the date, nature, and purpose of each disclosure to any person or agency. Enclosure (4) is designed for recording more than one disclosure and will be attached directly to the record.

(d) Disclosure accounting must be kept by the system of records Manager in accordance with the approved disposition for the related record, or for five years after disclosure is made (whichever is longer), per (e).

25 SEP 2012

(11) Administrative Remedies. Any individual affected adversely by a DON activity's violation of reference (a) and this Order may seek relief from the SECNAV through administrative channels. The individual shall first address the issue through the AC/S G-1 MCIEAST-MCB CAMLEJ Command PA Coordinator. If the complaint is not adequately addressed, the individual may contact the CNO (DNS-36) or Commandant of the Marine Corps (ARSF) for assistance.

(a) 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 refuses the individual's request for review of the initial denial of an amendment or, after review, wrongfully refuses 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 Record Keeping Standards. The activity fails to maintain an individual's record with accuracy, relevancy, timeliness, and completeness.

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

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

(c) Criminal and other Penalties. Reference (b) 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 PA information is at the discretion of each commanding officer 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 agencies should consider is prompt removal of authority to access information or systems from individuals who demonstrate egregious disregard or a pattern of error in safeguarding PA information.

1. Wrongful Disclosure Definition. Any member or employee of DON who, by virtue of his/her employment or position, has possession or access to records, and willfully makes a disclosure knowing that the disclosure is in violation of references (a) and (b) and this Order.

2. Maintaining Unauthorized Records Definition. Any member or employee of DON who willfully maintains a system of records for which a notice has not been approved, and not published in the Federal Register.

3. Wrongful Requesting or Obtaining Records Definition. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses.

(d) Litigation Notification. Whenever a complaint citing the PA is filed in a U.S. District Court against the DON (or any DON employee), the responsible DON activity shall promptly notify the CNO and provide a copy of all relevant documents. CNO (DNS-36) will notify the Defense Privacy Office (DPO), who shall apprise the Department of Justice. When a court renders a formal opinion or judgment, copies of the judgment and/or opinion shall be promptly provided to CNO (DNS-36). CNO (DNS-36) will apprise the DPO.

(12) Action. All military and civilian personnel shall familiarize themselves with this Order, and are responsible for complying with its content.

(13) Violations. A violation of this Order is punishable in accordance with the Uniform Code of Military Justice for military personnel. All other personnel will receive corrective or disciplinary action at the discretion of the CG and each commanding officer on a case-by-case basis.

5. Administration and Logistics. Not applicable.

6. Command and Signal

a. Command. This Order is applicable to MCIEAST-MCB CAMLEJ and its subordinate commands.

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



D. L. THACKER, JR.
Deputy Commander

DISTRIBUTION: A/B/C

25 SEP 2012

PA SELF-ASSESSMENT FORM

SECTION: _____ DATE: _____

This form is an internal document and is to be used by command leadership to assess the level of compliance in the handling of Personally Identifiable Information (PII) as delineated by law and or specific DoD/DON policy guidance. Some self-assessment items may not apply to your specific command. Where deficiencies are noted, the command should take immediate corrective action. For additional guidance and information go to the DON Privacy website at DONCIO.navy.mil or contact DNS-36 Privacy Act Officer at (202) 685-6546 or DON CIO Privacy Office at (703) 602-4412. This Self-Assessment form is an auditable record and should be kept on file for two years.

ADMINISTRATIVE

1. The name of your Privacy Act Manager is: _____

2. The name of the individual assigned to conduct this self-assessment is: _____

3. The command/department Privacy Act Manager has been identified in writing with clear roles and responsibilities identified.

 YES NO Who: _____

Reference: SECNAVINST 5211.5 E.7.h.--pg. 13

4. The command/department has an implementing Privacy Act instruction.

 YES NO Guidance Followed: _____

Reference: SECNAVINST 5211.5 E.7.h.--pg. 13

5. Are Privacy Act System of Records Managers knowledgeable of DON Privacy Act policy and procedures posted on DON website?

 YES NO How often is website viewed? _____

Reference: SECNAVINST 5211.5E 7.D. (3)-pg 11

6: Does command/department annually review the SORN listing?

 YES NO Date reviewed: _____

Reference: SECNAVINST 5211.5E 7.M (5)-pg17

7. Has the command/department disseminated guidance to its personnel on how to properly mark email, messages, letters, etc., that contain privacy act information prior to transmission?

 YES NO Method: _____

Reference: SECNAVINST 5211.5 E. 7.I(5)-pg.15

8. Are Privacy Act System of Records Managers trained on their responsibilities for protecting Privacy Act information being collected?

 YES NO Method? How often? _____

Reference: SECNAVINST 5211.5 E. 7.H.(5)-pg13

9. Has the command taken action to eliminate or reduce the need for the use of SSN's?

 YES NO What action: _____

Reference: SECNAVINST 5211.5 E 9.C.(6) - pg. 22

PAPER RECORDS

10. Does office use cross cut shredders that make documents unrecognizable?

 YES NO Type of Shredder: _____

Reference: SECNAVINST 5211.5E 8(b) - pg. 19

11. If command/department does not shred all documents containing privacy act information before being placed in a recycle container at random, spot check 10% of recycle containers within your organization to ensure that no privacy act information has been placed inside, awaiting disposal.

Number of containers checked: _____ Number of containers containing privacy information: _____ Method Used: _____

Reference: SECNAVINST 5211.5E 8.b(1) through (3) - pg.19

12. Do all forms that collect privacy act information directly from the individual contain a Privacy Act Statement?

 YES NO Forms Manager: _____

Reference: SECNAVINST 5211.5 E. 9.d.(1) - pg. 23

13. Does the command/department ensure that paper records are maintained in accordance with the disposition manual?

 YES NO Disposition: _____

Reference: SECNAVINST 5211.5 E 7.M.(14) - pg. 17

14. Does each unit Privacy Act System of Records Manager ensure files are not maintained illegally?

 YES NO How? _____

Reference: SECNAVINST 5211.5 E 7.M.(4) - pg 16

25 SEP 2012

15. Does the department Privacy Act Manager maintain liaison with records management officials?

YES NO Records Manager: _____

Reference: SECNAVINST 5211.5E 7.H.(9) - pg. 14

16. Do Privacy Act System of Records Managers ensure that all contractor personnel granted access to data maintained within his/her System of Records collection are properly trained and routinely inspected for Privacy Act compliance?

Records Manager: _____

Reference: SECNAVINST 5211.5E 7.M.(16)

17. Are Privacy Act System of Records Manager aware that there are regulations to be followed when making a disclosure and know where to find instructions for processing a request for disclosure?

Guidance followed: _____

Reference: SECNAVINST 5211.5E 8.A, 10, 13 pgs. 18, 24, 35

18. For static or electronic bulletin boards that disseminate command information to all hands or to select groups, check for the presence of privacy information. Privacy information should only be available to individuals with a need to know.

Number of boards checked: _____ Number of examples of where privacy information was found: _____

Reference: SECNAVINST 5211.5E 18.D.(6) - pg. 47

19. Does the command have protocols established to ensure privacy information is not inadvertently posted on a public or restricted access website?

YES NO Who reviews website: _____

Reference: SECNAVINST 5211.5E 7.D.(8) - pg. 11

20. Are command sponsored websites properly registered?

Number of sites: _____ Number properly registered: _____ Share Portal access checked against master list: _____

Reference: SECNAVINST 5211.5E 7.D.(10) - pg. 11

21. Spot check 25% of command websites searching for privacy act information that is available to individuals who do not have a need to know.

Number of sites checked: _____ Number of records with privacy information: _____ Share Portal access checked against master list: _____

22. Is documentation on file certifying all personnel have completed SORN training?

YES NO How is training completed/tracked? _____

Reference: SECNAVINST 5211.5E 7.M(3) - pg. 16, 59

23. Copy of SORN accessible for each system utilized by personnel.

YES NO Location: _____

Reference: SECNAVINST 5211.5E 7.M - pg. 16

24. Is documentation on file certifying all personnel have completed calendar year Privacy Act training?

YES NO How is training completed/tracked? _____

Reference: SECNAVINST 5211.5E 7.H(6) - pgs. 13, 59

Recommendations, comments or concerns:

25 SEP 2012

MCIEAST-MCB CAMLEJ PRIVACY ACT AND ROUTINE USE REQUEST FORM

Information contained on this form is maintained under the Systems of Records Notice NM05211-1 Privacy Act Request/Amendment Files and Tracking System (April 2, 2008, 73 FR 17959), and for official use only. **AUTHORITY:** under 5 U.S.C. 552a, The Privacy Act of 1974, as amended; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C., Headquarters, Marine Corps; E. O. 9397 (SSN). **PRINCIPLE:** Personal information gathered from the individual for the use of the Special Recognition Board. **PURPOSE:** This form is to provide personal information in association with the Special Recognition Board. **ROUTINE USE:** under U.S.C. 552 a (b) of the Privacy Act, and may be disclosed as routine use pursuant to 5 U.S.C. a (b). **DISCLOSURE** is VOLUNTARY, although awards may not be processed without this information.

Commanding General
Marine Corps Installations East-Marine Corps Base
Attn: G-1 (Privacy Act Coordinator)
PSC Box 20005
Camp Lejeune, NC 28542-0005

Date Requester completed the form (DD MMM YY)

(Please Check) Type of Request

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 and security clearance)

Information requested: (Describe information requested and where to locate the information)

If requesting a Military Police report Indicate if you are requesting the CLEOC report or all Documents. CLEOC ALL Documents

Requester or Client's Name: _____ SSN: (of subject) _____

Names of all persons involved: _____

Date of incident (DD MMM YY) : _____ Location of Incident: _____

Please provide your address: (Print or type clearly)

Name _____

Address (If military in barracks-provide Command Address) _____

City _____ State _____ Zip Code _____

How would you like to receive your records. PICK UP MAILED

I authorize a response via e-mail

(Requester's Name (PRINT)) _____

(Phone Number) _____

(Signature of Requester or agent)
(Signature required for PA/ROUTINE USE Requests)

AGENCY STAMP

"I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct".

PLEASE NOTE: There is no processing time limits when processing PA/ROUTINE USE requests, but we will process as expeditiously as possible. Depending on current workloads, information requested, dates and/or accidents etc...the response time may vary.

"FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE"

Any misuse or unauthorized release of personal information could result in both civil and criminal penalties.
You may return this request by faxing it back at (910) 451-3688 or e-mail to FOIA.MCBLejeune@usmc.mil

