



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

MCIEAST-MCB CAMLEJO 5211.6B  
G-1  
APR 16 2019

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

From: Commanding General  
To: Distribution List

Subj: PRIVACY ACT (PA)

Ref: (a) 5 U.S.C. §552a  
(b) SECNAV M-5210.1 Ch 1  
(c) SECNAVINST 5211.5E  
(d) SECNAVINST 5720.42G  
(e) MCIEASTO 5211.5  
(f) MCIEAST-MCB CAMLEJO 5720.1

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

Reports Required: I. Annual Privacy Act Report (Report Control Symbol  
MCIEAST-MCB CAMLEJ-5211.6-01), par 4b(2)(b)  
II. Unit Inspections (Report Control Symbol Exempt),  
par 4b(2)(b)  
III. Commanding General Evaluation Report (Report Control  
Symbol MCIEAST-MCB CAMLEJ-5040.6-01, par 4b(2)(b)  
IV. Privacy Act Self-Assessments (Report Control Symbol  
MCIEAST-MCB CAMLEJ-5211.6-01, par 4c(6))

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 reference (a), 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. MCIEAST-MCB CAMLEJO 5211.6A.

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 Record(s) (SOR) 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.

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

APR 16 2019

(2) Concept of Operations. All MCIEAST personnel shall fully comply with the requirements of references (a) through (f) in order to safeguard personal information resident in a SOR. 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 (b) provides appropriate instructions for retention and disposal of records.

b. Tasks

(1) 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 who shall:

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

(b) Appoint, in writing, a MCIEAST-MCB CAMLEJ PA Program Manager to administer the program.

(2) MCIEAST-MCB CAMLEJ PA Program Manager shall:

(a) Provide guidance and assistance to subordinate commands and staff departments.

(b) Collect and maintain rosters for the annual PA contact training, SOR Manager and user training, inspection results, and breach documents for MCIEAST-MCB CAMLEJ staff departments and MCIEAST subordinate commands.

(c) Update PA training materials and distribute annual PA training schedule notices and Systems of Records Notices (SORN) training via naval message and e-mail.

(3) MCIEAST Commanders and General and Special Staff Department Heads shall: Appoint, in writing, a PA Manager to maintain oversight of their PA program.

(4) PA Managers shall:

(a) Create and maintain a turnover binder that will contain, at a minimum, an updated desktop procedure, references, reports, inspection results, SORN listing, and points of contact (POC) listing.

(b) Issue implementing instruction and guidance that will, at a minimum, cover an annual review of the SORN listing, review of local order, reporting requirements, and program maintenance.

(c) Maintain a POC listing for PA personnel within the command and higher headquarters.

APR 16 2019

(d) Conduct internal inspections on an annual schedule, and conduct an internal self-inspection on the off years. Perform unannounced self-assessments visits to identify strengths and weaknesses and to determine the training needs of personnel who work with privacy records/information per reference (c). Maintenance and verification of the assessments is an inspectable item.

(e) Review all internal directives, procedures, internal controls, and forms (DD 67) for privacy implications.

(f) Review and update the listing of SORNs. The listing shall include the records retention and disposition instructions of each SORN maintained by the command.

(g) Ensure unpublished SOR on individuals are not being maintained, and no new or significantly changed system exists. Current authorized and published systems can be located on the Department of the Navy (DON) Chief Information Officer website: <http://www.doncio.navy.mil>. Annually review and update the SORN and publish a command SORN bulletin.

(h) Work closely with command officials to ensure 100 percent completion of the annual PA training for all military, civilian, and contractor personnel. Track and document training for all personnel who access other persons personally identifiable information maintained in a SOR. Use enclosure (1) to track group PA training sessions. Training certificates and rosters shall be maintained at the department-level for two years. Report annual training information to the Command PA Program Manager.

(i) Work closely with Department PA/SOR Managers to ensure appropriate processes are in place to minimize the misuse of personal data.

(j) Ensure official files retrieved by name or other identifiers are not collected or maintained without first ensuring a SORN exists that permits such collection.

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

(l) Ensure compliance is followed when including PA Statements (PAS) on forms per reference (c).

(m) 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."

(n) Ensure that only those Department of Defense (DoD)/DON officials with a "need to know" in the official performance of their duties have access to unrestricted information contained in a SOR per reference (d).

(o) Ensure records are kept in accordance with retention and disposal instructions set forth in reference (b).

(p) Report any suspected loss or compromise of personal data from a SOR in accordance with reference (e).

APR 16 2019

(q) Ensure at least one department/section self-assessment is completed annually and submitted to the Command PA Manager for review.

(r) Advise Headquarters, U.S. Marine Corps (HQMC) when the need to establish a new PA SOR exists; when an existing SOR needs to be amended, altered, or deleted; or if it is no longer required. The Department SOR Manager shall determine the relevancy and necessity of information during the development of a new SOR or when an amendment to an existing SOR is proposed.

c. Coordinating Instructions

(1) Training

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

(b) Reference (b) provides information on DON training programs and resources. Training materials and links are located on the MCIEAST-MCB CAMLEJ external website:

<http://www.mcieast.marines.mil/StaffOffices/Adjutant/PrivacyActProgram.aspx>

(c) Per reference (c), all individuals who work with a PA SOR shall receive SORN training annually. Advise and stress to individuals their rights and responsibilities in regards to 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 PA 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, or delete SORNs, contact the Chief of Naval Operations (CNO) (DNS-36)/Commandant of the Marine Corps (CMC) (ARSF) per reference (c).

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

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

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

APR 16 2019

(4) Recording of Statements Made in Person. Except when authorized by statute, regulation, other lawful authority, or manual verbatim transcriptions, 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 (c), 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 personnel who have an official need-to-know have access to the collected information. Detailed safeguards and exemption release information are provided on each SORN.

(6) PA Self-Assessment. 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. Use the self-assessment form in enclosure (2) to measure compliance with the PA program. PA Managers will retain self-assessment reports for two years or until the next self-assessment is completed per references (b) and (c).

(7) Breach Reporting. 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 could be adversely affected. Reporting of PA breaches will follow the guidance set forth in reference (e).

(8) Access to Records

(a) References (a) and (c) provide that individuals must be allowed access to records about themselves, pursuant to the 12 conditions of PA disclosure without consent provisions. The person seeking access to records about themselves may inspect the record, copy it, or be furnished a copy. In addition, they may designate another person to accompany them to review their record in the accompanying person's presence.

(b) All other requests for notification, access, or amendments to records held by each command should be in writing to each respective PA official. Access to records under the control of each installation can be requested from their PA Release Office. Requests for access will be acknowledged within 10 working days, with access provided within 30 days. Complete enclosure (3) to request PA documents from MCIEAST-MCB CAMLEJ.

(c) Amendment of Records and Statement of Disagreement

1. Amendment. Individuals have a right to request amendments 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

APR 16 2019

writing with proper documentation provided showing the record to be in error. The burden of proof rests with the individual. The SOR Manager does not have to agree. Should amendment of the record be denied, the decision is appealable.

2. Statement of Disagreement. The individual may submit a concise statement of disagreement listing the reasons for disagreeing with the refusal to amend.

3. Appeal Process. The appeal must be in writing and be received by the cognizant review authority (i.e., HQMC Manpower and Reserve Affairs, DON Office of the Judge Advocate General, Office of General Counsel, or Office of Personnel Management) within 60 calendar days of the date of the response. The appeal must include the denial letter and a statement of disagreement.

(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 release determination and redaction as required. The individual will be notified in writing if a record is referred to the FOIA office for release determination.

(b) PA Release Office. This office will process all PA requests for information in accordance with reference (c). Additionally, this office will maintain a complete administrative record to include a tracking database, response letters, referrals, releases, and records according to the retention schedule in reference (b). If release of documents is questionable, documents will be referred to the FOIA Officer for release determination as outlined in reference (d).

(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 (b) and (f), to the FOIA office 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 used). Responses to inquiries from sources outside the DoD about MCIEAST-MCB CAMLEJ personnel will be forwarded for release by the CG MCIEAST-MCB CAMLEJ (Attn: G-1, PA Coordinator).

(10) Disclosure Accounting

(a) Per reference (f), 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 the FOIA per reference (d). Personnel acting in their official capacity will present an authorization letter signed by a command official specifying the records sought to the SOR Manager in order to receive a copy of the official record.

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

APR 16 2019

(c) Enclosure (4) is an example of the disclosure accounting form. Each SOR 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 SOR Manager in accordance with the approved disposition for the related record or for five years after disclosure is made, whichever is longer, per reference (f).

(11) Administrative Remedies. Any individual affected adversely by a DON activity's violation of reference (a) and this Order may seek relief from the Secretary of Navy through administrative channels. The individual shall first address the issue to the MCIEAST-MCB CAMLEJ Command PA Coordinator. If the complaint is not adequately addressed, the individual may contact the CNO (DNS-36) or CMC (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 their 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 their 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, in some cases, attorney fees.

(c) Criminal and Other Penalties. Reference (c) authorizes criminal penalties against individuals for violations of its provisions, and each violation is punishable by fines up to 5,000 dollars. 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.

APR 16 2019

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

2. Maintaining Unauthorized Records Definition. Any member or employee of the DON who willfully maintains a SOR which a SORN has not been approved and is not published in the Federal Register.

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

(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 the CNO (DNS-36). The CNO (DNS-36) will apprise the DPO.

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

(13) Violations. A violation of this Order is punishable under 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 Commander on a case-by-case basis.

5. Administration and Logistics. Not Applicable.

6. Command and Signal

a. Command. This Order is applicable to MCIEAST, its subordinate commands, all MCIEAST-MCB CAMLEJ General and Special Staff departments, and the supported tenant commands on MCIEAST installations.

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

S. A. BALDWIN  
Deputy Commander

DISTRIBUTION: A/B/C



APR 16 2019

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

2. Maintaining Unauthorized Records Definition. Any member or employee of the DON who willfully maintains a SOR which a SORN has not been approved and is not published in the Federal Register.

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

(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 the CNO (DNS-36). The CNO (DNS-36) will apprise the DPO.

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

(13) Violations. A violation of this Order is punishable under 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 Commander on a case-by-case basis.

5. Administration and Logistics. Not Applicable.

6. Command and Signal

a. Command. This Order is applicable to MCIEAST, its subordinate commands, all MCIEAST-MCB CAMLEJ General and Special Staff departments, and the supported tenant commands on MCIEAST installations.

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

  
S. A. BALDWIN  
Deputy Commander

DISTRIBUTION: A/B/C

# TRAINING ROSTER

ENTER THE TYPE OF TRAINING HERE

Date: \_\_\_\_\_

EMPLOYEE NAME	EMPLOYEE WORK PHONE NUMBER	EMPLOYEE SIGNATURE	DEPARTMENT/SECTION

TRAINER'S NAME: \_\_\_\_\_ TRAINER'S SIGNATURE: \_\_\_\_\_

Enclosure (1)

MCI-EAST-MCB CAMLEJ/O 5211.6B  
APR 16 2019

APR 16 2019

# 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.(7)-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)-pg. 17

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.l.(6)-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)-pg. 13

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 illegally maintained?  
 YES  NO How? \_\_\_\_\_

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

APR 16 2019

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

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)-pg. 13

Recommendations, comments or concerns:

**MCIEAST-MCB CAMLEJ**  
**FREEDOM OF INFORMATION ACT/PRIVACY ACT REQUEST FORM**

**PRIVACY ACT STATEMENT**

Information contained on this form is maintained under the Systems of Records Notice NM05720-1 FOIA Request/Appeal Files and Tracking System (April 2, 2008, 73 FR 17981) 5 U.S.C. 552, the Freedom of Information Act, as amended. AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; E.O. 9397 (SSN); and Secretary of the Navy Instruction 5720.42F, Department of the Navy Freedom of Information Act Program. PRINCIPLE: Individuals who request access to information under the provisions of the Freedom of Information Act (FOIA) or make an appeal under the FOIA. 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. ROUTINE USE: 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 the DoD as pursuant to 5 U.S.C. 552a(b)(3). DISCLOSURE: MANDATORY for computer matching.

**MAILING ADDRESS:**

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

For more information please visit:

FOIA Service Center

Date REQUESTER completed this form: \_\_\_\_\_

Date Received: \_\_\_\_\_

MCIEAST-MCB CAMLEJ20 \_\_\_\_\_

You may return this request by faxing it back at (910) 451-1265 or e-mail to FOIA.MCIEAST@usmc.mil

**FREEDOM OF INFORMATION ACT (FOIA)**

Police reports (On other parties), Command Investigations, Command Records (Not Individual based), video viewing

**PRIVACY ACT (PA)**

Personal information directly about the individual, SRB, OPM, Military Police records (on Self)

**ROUTINE USE: OFFICIAL USE ONLY**

Federal, State and local agency for civil or criminal or for hiring, retention, Insurance Company, accident report, security clearance and contract

I am willing to pay the fees above \$15.00 for the processing of my request in the amount of: (if required) \_\_\_\_\_

Case Information: (Print or type clearly)

PMO Records Indicate:

Information requested:

(Describe information requested and where to locate the information)

CLEOC (Electronic Report)  All Documents

Requester or Client's Name (if other than requester): \_\_\_\_\_ SSN: (required for search) \_\_\_\_\_

Names of all persons involved: (if known) \_\_\_\_\_

Date of incident (DD MMM YY): \_\_\_\_\_ Location of incident: \_\_\_\_\_

Requester Contact Information: (Print or type clearly)

Rank: \_\_\_\_\_ Name: \_\_\_\_\_ Unit/Organization: \_\_\_\_\_

Mailing Address: (Required for processing) \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Do you want to pick up the report or have it mailed to you?  PICK UP  MAILED  E-MAIL \_\_\_\_\_

Not an Official Government e-mail address

(Requester's Name (PRINT) \_\_\_\_\_

(Phone Number) \_\_\_\_\_

(Signature of Requester or agent)  
(Signature required for processing)

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

**PLEASE NOTE:** This office has twenty (20) working days in which to provide a response to a FOIA Request.

Depending on current workloads, information requested, dates and/or accidents etc...the response time may vary.

Reset Form

Submit by Email

# 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