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

MCIEASTO 5211.1C
G-1

MARINE CORPS INSTALLATIONS EAST ORDER 5211.1C

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 3040.1D
(f) MCIEASTO 5720.1A
(g) ALNAV 070-07 of 4 Oct 07
(h) MCIEASTO 5211.5

Encl: (1) MCIEAST Freedom of Information Act/Privacy Act and Routine Use Request Form
(2) Disclosure Accounting Form
(3) Record of Disclosure/Consent Authorization Form
(4) General Purpose Privacy Act Statement

1. Situation. 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. Cancellation. MCIEASTO 5211.1B.

3. Mission

a. 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 (MCIEAST).

b. Summary of Revision. This Order has been revised and should be reviewed in its entirety.

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

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) All personnel within MCIEAST shall fully comply with the requirements of references (a) through (h) 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.

(b) 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.

(2) Concept of Operations. This program shall reduce administrative burden, and to promote and improve paperwork efficiency. All MCIEAST Commanders, General and Special Staff Department Heads shall:

(a) ensure PA information (home address, date of birth, social security number (SSN), credit card or charge card account numbers, etc.) pertaining to a service member, civilian employee (appropriated and non-appropriated fund), military retiree, family member, or another individual affiliated with the activity (e.g., volunteers) is protected from unauthorized disclosures;

(b) ensure official files retrieved by name or other identifier are not maintained on individuals without first ensuring a system of records notice exists that permits such collection;

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

(d) review internal directives, forms, websites, share portals, practices, and procedures, including those where Privacy Act Statements (PAS) or PA information is solicited;

(e) maintain liaison with records management officials (forms and reports, etc.) regarding the maintenance and disposal procedures and standards, as appropriate;

(f) oversee the administration of the MCIEAST PA program, review and resolve PA complaints, develop a privacy education, training and awareness program;

(g) review Privacy Impact Assessments (PIA) for appropriate System of Records Notice;

(h) ensure the senior-level individual, or their designated representative who has been appointed in writing, reports PA SORN breaches, including higher headquarters on the notification. The PA Coordinator will maintain a copy of all breach reports for awareness and record keeping purposes;

(i) process all PA requests for information under 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 (d). Refer documents to the Freedom of Information Act (FOIA) Officer for release determination if documents are determined questionable, as outlined in reference (f);

(j) conduct and document privacy awareness training for activity personnel (military, civilian, contractor, volunteers, non-appropriated fund employees, etc.). Training options include: “All Hands” awareness briefing, staff memos, formal training, and circulation of brief sheet on Best Practices, etc;

(k) mark all documents that contain PA information (letters, memos, e-mails, messages, documents, faxes, etc.) FOR OFFICIAL USE ONLY (FOUO). 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;” and

(l) ensure supervisors conduct spot checks within their assigned area of responsibility (AOR), per reference (g).

b. Subordinate Element Missions

(1) MCIEAST Assistant Chief of Staff, G-1 (AC/S G-1) shall:

(a) be designated and appointed in writing as the PA Officer for MCIEAST;

(b) serve as the principal point of contact on PA matters; and

(c) appoint in writing a PA Coordinator to administer the PA Program.

(2) PA Coordinator shall:

(a) 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;

(b) work closely with command officials to conduct annual PA training as well as systems of records training; and

(c) ensure all PA system of records Managers have a copy of the appropriate PA systems notice and understand PA rules.

(3) MCIEAST Subordinate Commanders shall:

(a) appoint a PA Officer in writing at their respective commands to administer and supervise the execution of this Order within their AOR;

(b) notify all personnel within their command of the provisions of this policy;

(c) address steps and potential risk factors, necessary to ensure that PA information is not compromised;

(c) receive all subordinate commands PA Breach reports and maintain records of such breaches; and

(d) receive PA training reports and spot checks from subordinate commands, consolidate and submit to higher headquarters as requested.

(4) Command PA Officers/PA Coordinators shall:

(a) be appointed in writing to assist with the PA program;

(b) advise the MCIEAST PA Officer and Coordinator promptly of the 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; and

(c) ensure supervisors conduct spot checks within their assigned AOR, per reference (g).

c. Coordinating Instructions

(1) Responsibility. All military and civilian personnel are responsible for the administration and supervision of the PA within their AOR. In accordance with published instructions from higher authority are required to:

(a) ensure PA information contained in a system of records to which they have access or are using to conduct official business, is protected so 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 system 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 PA information contained in a system of records;

(f) not maintain privacy sensitive information in public folders;

(g) report any unauthorized disclosure of PA information from a system of records to the applicable PA Officer for his/her activity; and

(h) report the maintenance of any unauthorized system of records to the applicable PA Officer for his/her activity.

(2) Training. 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 (h), and this Order.

(3) Breach Reporting

(a) 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

1. The process outlined below 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 PA Officer or Coordinator by telephone or breach report.

2. Within one hour of the discovery, complete and send the Initial Breach Report per reference (b).

3. Within 24 hours, provide an after action report to include lessons learned per reference (b).

(4) PA Enforcement Actions

(a) Administrative Remedies. Any individual affected adversely by a Department of the Navy (DON) activity's violation of reference (a) and this Order may seek relief from the Secretary of the Navy (SecNav) through administrative channels. The individual shall first address the issue though the PA Coordinator having cognizance over the relevant records or their 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 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 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 the 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.

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

(d) 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.

(e) 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.

(5) Federal Register Notice of System of Records. In line with one of the basic principles of the PA, no records will be 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 systems notices in the Federal Register. References (a) and (b) provide the method for establishing and modifying system of records.

(6) Safeguarding of Information. The PA requires that personal information collected on an individual must be safeguarded. Thus, those who use or create a system of records which contain personal information about another individual are responsible for safeguarding that information, ensuring that only those who have a need to know in their official capacity have access to it. References (a) and (b) provide further instructions for safeguarding of information.

(7) Access to Records

(a) Per references (a) and (b), individuals must be allowed access to records about themselves, except where specific exemption has been approved by the 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 it is in error. 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 so that another individual’s record is not inadvertently disclosed.

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

(c) Routine requests for access to their service record book/officer qualification record (SRB/OQR) from military personnel who are assigned to MCIEAST will be honored at the reporting unit level, then the command level. Information in the Marine Corps Total Force System is periodically audited and requires the presence of the individual to ensure accuracy. Additionally, Marines are encouraged to review their SRB/OQR periodically to ensure accuracy of its contents. Written access to these records is not required.

(d) All other requests for notification, access, or amendments to records held by each command should be in writing to each respective PA Officer. Requests for access will be acknowledged within ten working days, and access provided within 30 days. Enclosure (1) may be used for requesting information.

(8) 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) Denial Authority

(a) Reference (b) delegates authority to the Commanding General (CG), MCIEAST to deny requests for notification, access and amendment to records when such records relate to matters within the CG’s AOR. This authority has been sub-delegated to the AC/S G-1.

(b) There are occasions when denial is appropriate, however only the CG or a designated

representative has the authority to do so. If there is a need to deny an individual access to information about themselves currently maintained in a system of records utilized by MCIEAST, the system of records manager will refer the request to the AC/S G-1 for release determination. The system of records manager must provide complete justification for the denying access.

(10) Disclosure. A first party access request will be submitted to the command's PA Officer for collection and release using enclosure (1). Documents containing information pertaining to the requester and other parties will be referred pursuant to reference (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 personnel will be forwarded for release by the CG MCIEAST (Attn: G-1 PA Coordinator).

(11) 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) Enclosures (2) and (3) are samples of disclosure accounting records. 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 (2) is designed for recording more than one disclosure and will be attached directly to the record. Enclosure (3) lists the minimum required information, such as name and address of the person or agency to whom the disclosure was made, and the individual's consent to release the authorized information.

(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) according to reference (e).

(12) The purpose of the accounting requirement is to:

(a) allow individuals to determine to whom their records have been disclosed;

(b) provide a basis for subsequently advising recipients of records of any disputed or corrected records; and

(c) provide an audit trail to ensure compliance within the activity.

(13) 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. It is essential that the information collected and maintained is relevant, timely, complete, and up to date. The PA authorizes civil action against an agency for failure to maintain records accordingly.

(b) The PA requires any form, questionnaire, report, or other media used to collect data from employees must be accompanied by a PAS (enclosure (4)). 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, and also provide administrative instructions concerning the use of the general purpose PAS.

(d) 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.)

(14) 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 in accordance with reference (e).

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

(16) 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.

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

W. A. MEIER
Chief of Staff

DISTRIBUTION: A