DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

CNICINST 5211.1
N00C

FEB 3 2009

CNIC INSTRUCTION 5211.1

From: Commander, Navy Installations Command

Subj: PRIVACY PROGRAM

Ref: (a) SECNAVINST 5211.5E
(b) Title 5, United States Code, Section 552a
(c) DoD Directive 5400.11, "DoD Privacy Program," May 8 2007
(d) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(e) E-Government Act of 2002 (Public Law 107-3347) of December 17, 2002
(f) ALNAV 070/07 of 042232Z Oct 07
(g) DON CIO Washington DC 291652Z FEB 08

Encl: (1) Definitions

1. Purpose. To implement reference (a), issue policies and procedures, and assign responsibilities for the administration of a Commander, Navy Installations Command (CNIC) Privacy Program, in accordance with references (a) through (g).

2. Scope. This instruction applies to all CNIC activities that collect, maintain, use or disseminate personally identifiable information (PII) contained in a Privacy Act (PA) system of records to accomplish the CNIC mission. This includes military, civilian and contractor personnel who collect, maintain and disseminate PII in the course of their official duties, and vendors who develop, procure or use information technology (IT) systems to collect, maintain, or disseminate PII from or about members of the public. In case of a conflict, the provisions of references (a) through (d) take precedence over other existing Navy or command directives that deal with the privacy and rights of individuals in regards to their personal records.

3. Policy. Consistent with references (a) through (g), it is CNIC policy to:

a. Ensure that all personnel comply fully with PA requirements to protect the privacy of individuals from unwarranted invasion.

b. Collect, maintain, safeguard, and use only that personal information needed to support a Navy function or program as authorized by law or Executive Order, and disclose this information only as authorized by references (a) and (b).

c. Retain personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

d. Grant individuals access to and copies of all or any portions of their records, subject to authorized exemption procedures.

e. Allow individuals to request amendment of their records when discrepancies prove to be erroneous, untimely, incomplete or irrelevant.

f. Allow individuals to request an administrative review of decisions that deny them access to or amendment of their records.

g. Ensure that adequate safeguards are in place to prevent misuse, unauthorized disclosure, alteration or destruction of personal information in records.

h. Ensure that records describing how an individual exercises his or her rights guaranteed by the First Amendment (freedom of religion, speech and press, peaceable assembly, and petition for redress of grievances) are not maintained, except as authorized by reference (b).

i. Ensure that only systems of records which have been published in the Federal Register are maintained.

4. Responsibilities

a. Commander, Navy Installations Command shall:

(1) Implement a Privacy Program.

(2) Appoint a Command Privacy Act Coordinator to administer the Privacy Program at CNIC Headquarters.

b. CNIC Privacy Act Coordinator. The CNIC Privacy Act Coordinator is responsible for administering the Privacy Program and shall:

(1) Serve as the principal point of contact on all privacy matters.

(2) Ensure all systems of records subject to reference (b) are described by published systems of records notices (SORN); that systems of records are not modified or otherwise expanded prior to complying with reporting and public notice requirements; and that disclosure of personal information and accounting records is maintained in accordance with references (a) and (b).

(3) Maintain liaison with Department of the Navy (DON) Privacy Officials, as appropriate, for the publication of systems of records notices and Privacy Impact Assessments (PIA), the DON Privacy Training Program, breach notification procedures, annual privacy reports and data calls, and all other privacy matters.

(4) Maintain liaison with records management officials, as appropriate, regarding maintenance and disposal of systems of records, standards, forms, reports, etc.

(5) Provide training to CNIC systems managers and personnel involved in any aspect of maintaining systems of records on the provisions of references (a) and (b) and their responsibilities for safeguarding PII.

(6) Ensure privacy training is conducted that includes orientation training, specialized training, management training and system manager training, and that all CNIC personnel are aware of their roles and responsibilities under the provisions of references (a) and (b).

(7) Review internal directives, practices and procedures, including those having privacy implications, for compliance with references (a) and (b).

(8) Review and validate proposed PIAs to ensure privacy implications have been identified and evaluated, and submit the validation to appropriate DON Privacy Officials.

(9) Consult with appropriate legal authorities, as needed.

(10) Provide policy guidance for processing requests made under the PA and applicable exemptions.

(11) Ensure PA requests are processed in accordance with references (a) and (b).

(12) Process PA complaints.

(13) Conduct staff assistance visits or program evaluations within CNIC and subordinate activities to ensure compliance with requirements and provisions of references (a) and (b).

(14) Implement protocols and develop administrative tools to avoid the loss of PII.

(15) Work with the Public Affairs Officer (PAO) and Webmaster to ensure PII is not placed on public Web sites or in public folders.

(16) Report loss or suspected loss of PII to the appropriate authorities, take immediate action to notify affected individuals, and take steps to mitigate any damage caused by the loss of data.

c. CNIC Staff Judge Advocate shall:

(1) Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the PA.

(2) Review proposed denials of PA requests.

d. CNIC Information Officer (IO) shall:

(1) Integrate the protection of PII into the IT systems management process in accordance with reference (e).

(2) Ensure PIAs are conducted on IT systems that collect or maintain PII or any IT system or application that may have privacy risks.

(3) Review and validate proposed PIAs to ensure compliance with Department of Defense (DoD) information assurance policies.

(4) Provide guidance to program managers and system managers during the preparation and review of PIAs.

(5) Implement DON IT privacy requirements in accordance with reference (a).

e. CNIC Regions shall:

(1) Issue an implementing instruction and ensure a Privacy Program is implemented throughout their regions.

(2) Appoint a Region PA Coordinator to administer the Privacy Program who shall:

(a) Serve as the principal point of contact for all privacy matters.

(b) Ensure no official files are maintained on individuals that are retrieved by name or other personal identifier without an existing system of records that permits the collection.

(c) Maintain liaison with CNIC PA Coordinator and other PA Coordinators throughout their regions.

(d) Provide to the CNIC PA Coordinator a complete listing of all PA Coordinators under their jurisdiction, which will include activity name, name of PA Coordinator, mailing address, E-mail address, office code, commercial and DSN telephone numbers, and fax numbers.

(e) Maintain liaison with records management officials, as appropriate, regarding maintenance and disposal of systems of records, standards, forms, reports, etc.

(f) Ensure privacy training is provided to activity/command personnel that includes orientation training, specialized training, management training and system manager training, and ensure that all personnel are aware of their roles and responsibilities for safeguarding PII under the provisions of references (a) and (b).

(g) Review internal directives, forms, practices and procedures to ensure compliance with references (a) and (b).

(h) Ensure PA requests are processed in accordance with references (a) and (b).

(i) Process PA complaints.

(j) Conduct annual reviews of systems of records to ensure necessity, accuracy, and completion.

(k) Implement protocols and develop administrative tools to avoid the loss of PII.

(l) Work with the PAO and Webmaster to ensure PII is not placed on public Web sites or in public folders.

(m) Report loss or suspected loss of PII to appropriate authorities, take immediate action to notify affected individuals, and take steps to mitigate any damage caused by the loss of data.

f. CNIC System Managers shall:

(1) Review reference (a) to ensure they are fully cognizant of their responsibilities for overseeing the collection, maintenance, use and dissemination of information from a system of records.

(2) Establish administrative, technical and physical safeguards to ensure each system of records is protected from unauthorized alteration, destruction and disclosure; and protect against any reasonably anticipated threat or hazard that may result in substantial harm, embarrassment, inconvenience or unfairness to individuals on whom records may be maintained.

(3) Identify all systems of records under their cognizance and ensure that access to each system of records is limited to only those DoD/DON personnel with an official need-to-know.

(4) Ensure that all personnel who have access to systems of records or who develop or supervise procedures for handling such records are aware of their responsibilities and are properly trained to safeguard PII.

(5) Ensure that official files on individuals, which are retrieved by name or other personal identifier, are not maintained without first ensuring that a notice for the system of records has been published in the Federal Register.

(6) Prepare any required new, amended or altered system of records notices and submit them through the local PA Coordinator to the DON Privacy Office, Chief of Naval Operations (Director, Navy Staff - 36)(CNO (DNS-36)), for review and submission for publication in the Federal Register.

(7) Perform an annual review on each system of records notice under their cognizance to determine accuracy and relevancy, and submit any changes to the DON Privacy Office, CNO (DNS-36).

(8) Consult the local PA Coordinator when initiating the use of new forms that request or contain PII to ensure a Privacy Act Statement is provided and complies with the requirements of reference (a), and that a system of records notice is identified for the authority for the collection of PII.

(9) Ensure that no record contained in a system of records is disclosed, except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains.

(10) Maintain a disclosure accounting form for each record in a system of records made without the consent of the subject of the record, except those made within DoD on an official need-to-know basis or those made under the provisions of the Freedom of Information Act (FOIA).

(11) Work closely with IT personnel to identify any new information systems being developed that contain PII, and complete and maintain a PIA for those systems that collect, maintain or disseminate PII to address privacy factors and risks in accordance with reference (a).

(12) Ensure that records contained in a system of records are maintained in accordance with the identified systems of records notice and DON requirements for retention and disposal.

(13) Ensure adequate safeguards are in place to protect PII where personnel are authorized to work from home, to include: compliance with references (a) and (b) and the applicable system of records notice; a policy on limiting the amount of PII personnel may possess at home; the use of password protection on government and computers; the use of physical safeguards, such as, locking cabinets, drawers or safes; and any

additional administrative, technical and physical safeguards as necessary to safeguard PII.

5. CNIC Systems of Records Notices. CNIC systems of records notices shall be reviewed annually for accuracy and relevancy. The PA Coordinator is the point of contact for CNIC systems of records notices and shall be notified prior to the initiation of a new system of records. CNIC systems of records notices may be viewed at the CNIC Gateway Privacy Act page, https://cnicgateway.cnic.navy.mil/HQ/N00/CAPM/PAP/default.aspx.

6. PII Spot Checks. In accordance with reference (f), CNIC supervisors shall ensure that PII Spot Checks are conducted for their assigned areas of responsibility, focusing on areas that deal with PII on a regular basis to ensure basic safeguards are in place. Spot checks shall be conducted on a semi-annual basis and action should be taken immediately to correct any weaknesses identified. Completed spot check forms are auditable records and shall be submitted to the local PA Coordinator.

7. Privacy Training. Privacy training is mandatory for all CNIC personnel (military, civilian, and contractor) and shall be completed annually. Total Workforce Management System (TWMS) is the official CNIC database for total workforce training and is the preferred tool for privacy training. All CNIC personnel are responsible for ensuring individual annual privacy training requirements are met. The PA Coordinator is the point of contact for privacy training and shall ensure training courses are current and relevant, and that records of completion are maintained.

8. Requests for Access to Records or Amendment of Records. A written acknowledgement of a request for access to or amendment of a record will be made within 10 working days of receipt of the request. The individual will be advised of the final decision or action on the request within 30 working days of receipt of the request.

9. Responding to Requests for Access to Records. Prior to granting access to records, the system manager will take the following action, as appropriate:

a. Ensure the request was made in compliance with the "Record Access Procedures" outlined in the applicable system of records notice (e.g., provides full name and is signed).

b. When a request is made in person, the individual will be asked to provide verification of identity (i.e. state or federally issued identification card, driver's license or military identification card). An individual may by accompanied by a person of his or her choice when reviewing a record, if written authorization to do so is provided by the individual.

c. Direct a search of the system of records to determine whether the system contains a record pertaining to the individual.

d. If the record which is the subject of the inquiry exists within the system, the system manager will determine whether the record should be exempted from the requirement to give the individual access per reference (a).

e. If the record cannot be properly exempted, the requester will be notified in writing and a copy of the record will be made available, unless the record was compiled in anticipation of litigation or contains classified information pursuant to reference (a).

10. Responding to Requests to Amend Records. Amendments under this instruction are limited to correcting factual matters. When records sought to be amended are covered by another directive, the administrative procedures under that directive must be exhausted prior to invoking the PA. The appropriate local system manager will act on requests to amend records. If the system manager determines that any portion or all of a request to amend a record is not warranted, the request, recommendation and related information (including a copy of the record that is the subject of the request) will be forwarded to the denial authority.

11. Denial of Access to Records

a. Only a denial authority may deny access to a record pertaining to an individual.

b. Within the CNIC enterprise, only the Commander, Navy Installations Command, Regional Commanders, and Installation Commanding Officers are designated denial authorities, authorized to deny access to information in a system of records under an exemption cited in the systems notice. A denial authority may specifically delegate this authority in writing to other officials as deemed appropriate.

c. Pursuant to reference (a), a denial may only be made if the record was compiled in reasonable anticipation of civil action, the systems notice identifies a specific exemption for the record, the record contains classified information that has been exempted under one of the DoD blanket exemptions, or access to the record may be denied based on some other federal statute.

d. Should the system manager propose denial of a request for access, the request, recommendation and related information will be forwarded to the denial authority. This information must be forwarded in a timely and expeditious manner in order to provide a response to the individual within the 10-working-day limitation.

e. If the denial authority concurs with the recommendation for exercise of an exemption, a formal denial will be made promptly notifying the requesting individual of the determination, and a copy of the denial letter will be forwarded to the DON Privacy Officer, CNO (DNS-36).

f. Formal denials of access to records must be in writing and include at a minimum:

(1) The name, title or position, and signature of the designated denial authority;

(2) The date of the denial;

(3) The specific reason for the denial, including specific citations to the applicable sections of the PA, other statutes, DoD or DON Regulations, or Code of Federal Regulations (CFR) authorizing the denial;

(4) Notice of the individual's right to appeal the denial; and

(5) The title and address of the PA appeals official: Department of the Navy, Office of the General Counsel, ATTN: FOIA/PA Appeals Office, 1000 Navy Pentagon Rm. 4E635, Washington, DC 20350-1000.

g. If the denial authority determines that the exemption will not be exercised, access will be granted as requested.

12. Disclosure Accounting

a. A disclosure accounting is required for all disclosures of records maintained in a system of records, except those made to DoD personnel for use in the performance of their official duties and those made under the provisions of the FOIA.

b. A disclosure accounting, if required, will be maintained for the life of the record to which it pertains or for at least five years after the date of the disclosure for which the accounting is made, whichever is longer.

c. System managers will provide all information in the disclosure accounting to an individual requesting such information concerning their records, except entries pertaining to disclosures made for law enforcement purposes under paragraph 14 of reference (a) and when the system of records has been exempted from the disclosure requirement.

13. Fee Provisions

a. Pursuant to reference (a), a request for a copy of a record contained in a system of records is subject only to the direct cost of reproduction. Normally, only one copy of any record or document will be provided. A fee will not be assessed when the request is made to review the record and not to obtain a copy of the record, and the only means of allowing a review is to make a copy. For example, the record is stored in a computer and a copy must be printed to provide access or the system manager does not wish to temporarily surrender the original record for review.

b. Fees for the reproduction of documents or microfiche will be charged at the same rate as the fees charged under the FOIA schedule.

c. Per reference (a), a requestor is entitled to the first 100 pages of duplication free of charge. Fees are automatically waived if the direct cost of reproduction is less than $15.00. A decision to waive or reduce fees will be made on a case-by-case basis. Fee payment must be made by check or money order payable to the Treasurer of the United States. The individual will be notified of assessable costs at the time the records are released and advised to submit payment within 30 days.

14. Records Disposal. Records from a system of records are to be disposed of in such a way as to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction,

such as by tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation. Magnetic media may be cleared by completely erasing, overwriting, or degaussing the recording surface.

15. Loss or Suspected Loss of PII. In accordance with reference (g), known or suspected breaches or loss of PII shall be reported as follows:

a. CNIC personnel (military, civilian and contractor) who discover a known or suspected breach or loss of PII shall immediately report the incident to their supervisor.

b. Supervisors shall report the breach incident to their respective PA Coordinators. Incidents at CNIC HQ shall be reported to the CNIC PA Coordinator at 202-433-0895 or CNICHQ_Privacy@navy.mil. CNIC Region supervisors shall report breach incidents to their respective Region PA Coordinators.

c. The PA Coordinator is the official responsible for reporting breaches and will serve as the point of contact for follow-up actions and individual notifications, if applicable.

d. The PA Coordinator shall report the breach within one hour utilizing OPNAV 5211/13, DON Breach Reporting Form. A copy of the initial report must be submitted to the CNIC PA Coordinator at CNICHQ_Privacy@navy.mil. The initial breach report shall include the following information:

(1) Component/organization involved;

(2) Date of incident;

(3) Number of individuals impacted;

(4) Whether the individuals are government civilian, military, and/or private citizens (include a percentage of each category);

(5) Brief description of the incident, including the circumstances;

(6) Type of information lost or compromised; and

(7) Whether the PII was encrypted or password protected.

e. If commission of a crime is suspected, the PA Coordinator shall notify the local Naval Criminal Investigative Service (NAVCRIMINVSERV) Office to conduct an investigation.

f. Government Authorized Credit Card or financial data associated with the card - the PA Coordinator shall immediately notify the issuing bank and the CNIC Government Credit Card Manager.

g. If applicable, issue a Special Incident Report (OPREP3), in accordance with OPNAVINST 3100.6H.

h. The DON CIO Privacy Office will review the initial incident report within 24 hours, determine the potential risk of harm to impacted personnel, and notify the CNIC PA Coordinator of any required notifications.

i. Notifications, if required, are to be made within ten working days of the discovery of loss or suspected loss of PII. The notification shall be made via written letter or digitally signed email to all impacted individuals, and shall be signed by a senior official. If the ten day requirement is not met, the PA Coordinator must notify the DON CIO Privacy Office and provide the reason why notification was not made and what actions are being taken to complete the notification process. In all cases of notification the command/activity must investigate whether DON policy was followed, and in cases where policy was not followed, take disciplinary action weighing mitigating circumstances and severity of loss of PII.

j. PA Coordinators shall submit OPNAV 5211/14, After Action Reporting Form, to the DON CIO Privacy Office to provide additional information following the breach as soon as it becomes available. Submit a copy of the after action report to the CNIC PA Coordinator at CNICHQ_Privacy@navy.mil.

k. For impacted personnel who are difficult to locate, use any means that will likely succeed, such as establishing a Toll-free number or call center. The DON CIO website has more information, http://www.doncio.navy.mil/TagResults.aspx?ID=36.

l. As soon as possible but no later than 30 working days after the discovery of the breach - the PA Coordinator must submit another after action report, OPNAV 5211/14, to provide information to the DON CIO Privacy Office on remedial actions taken to prevent reoccurrence, individual notification status, whether notifications were required, lessons learned and

disciplinary action taken, where appropriate. Submit a copy of the after action report to the CNIC PA Coordinator at CNICHQ_Privacy@navy.mil.

16. Action. All personnel who are assigned specific duties and responsibilities by this instruction or who are involved in maintaining PII as prescribed by reference (a) will adhere to the guidance prescribed herein.

17. Point of Contact. The point of contact for all privacy matters shall be the CNIC Privacy Act Coordinator at (202)433-0895 or CNICHQ_Privacy@navy.mil.

M. D. PATTON
Captain, U.S. Navy
Chief of Staff

Distribution:
Electronic only, via CNIC Gateway
https://cnicgateway.cnic.navy.mil/HQ/N00/CAPM/DIRPR/default.aspx

Copy to:
CNO (DNS-36)

Definitions

1. Access. The review or copying by any individual of a record, or parts thereof, that is contained in a Privacy Act system of records.

2. Denial Authority. An official having cognizance over an exempt PA system of records who is authorized to deny access to information in those records under exemptions cited in the PA systems of records notice. The denial authority may also deny requests to amend a record contained in a system of records or to deny notification that a record exists.

3. Disclosure. The transfer of any personal information about an individual from a system of records, by any means of communication, to any person, private entity, government agency, other than the subject of the record, the subject's designated agent or legal guardian.

4. Individual. A living citizen of the U.S. or an alien lawfully admitted to the U.S. for permanent residence. The custodial parent of a minor or the legal guardian of any individual also may act on behalf of and individual. Members of the United States Armed Forces are "individuals." Corporation, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

5. Individual Access. Access to information pertaining to the individual by the individual or his/her designated agent or legal guardian.

6. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information.

7. Maintain. Includes maintain, collect, use, or disseminate.

8. Official Use. This term encompasses those instances in which Department of the Navy (DON) officials and employees have a demonstrated need for the use of any record, or the information contained therein, in the performance of their official duties.

9. Personal Information. Information about an individual that identifies, relates, or is unique to, or describes him or her (e.g., SSN, age, military rank, civilian grade, martial status,

race, salary, home phone numbers, etc.) as distinguished from information related solely to the individual's official functions or public life.

10. Personally Identifiable Information (PII). Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, SSN, or biometric records.

11. Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual that are located in a system of records. The request must be made in writing, be signed, and cite, or reasonably imply, that it is made pursuant to the Privacy Act.

12. Privacy Impact Assessment (PIA). An ongoing assessment to evaluate adequate practices in balancing privacy concerns with the security needs of an organization, and to guide owners and developers of IT systems in assessing privacy issues through early stages of development. The process includes privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by a designated privacy representative.

13. Record. Any item, collection, or grouping of information about an individual that is maintained by a DON activity including, but not limited to, the individual's education, financial transactions, and medical, criminal or employment history, and that contains the individual's name or other identifying particulars such as finger or voice print or a photograph.

14. Routine Use Disclosure. A disclosure of a record made outside the Department of Defense (DoD) for use that is compatible with the purpose for which the record was collected and maintained by the DoD. The routine use must have been included in the notice for the systems of records published in the Federal Register.

15. System Manager. An official who has overall responsibility for a system of records. He/she may serve at any level in DON.

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

17. System of Records Notice (SORN). A notice that informs the general public of the data being collected, used and maintained in PA systems of records, delineates the types of data being collected and on whom, provides the authority for the collection and procedures on how individuals may access the records, and sets the rules that DON will follow in collecting, maintaining, disseminating and disposing of the records. Each SORN is published in the Federal Register.