DEPARTMENT OF THE NAVY
COMMANDER NAVY REGION SOUTHWEST
937 NO. HARBOR DR.
SAN DIEGO, CA 92132-0058

IN REPLY REFER TO:
COMNAVREGSWINST 5211.1
N05H
24 JUL 2006

COMNAVREGSW INSTRUCTION 5211.1

Subj: REGIONAL PRIVACY ACT PROGRAM

Ref: (a) SECNAVINST 5211.5E
(b) SECNAV M-5210.1 (Records Management Manual)

Encl: (1) Privacy Program Terms and Definitions
(2) Appointing Letter, Designating Regional PA Coordinator/Command/Program PA Point of Contact
(3) Self-Assessment Checklist of Recommended PA Actions

1. Purpose. To ensure all military personnel and civilian/contractor employees are made fully aware of their rights and responsibilities under the provisions of the Privacy Act (PA); to balance Commander, Navy Region Southwest (CNRSW) need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy stemming from collection, maintenance, use, and disclosure of Protected Personal Information (PPI); and to assign responsibilities, coordination and implementation of the privacy management practices and procedures for the CNRSW PA program. PA definitions and terms are contained in enclosure (1). For additional definitions and terms, see reference (a).

2. Scope. This instruction applies to all Navy Region Southwest (NRSW) installation commands and functional programs.

3. Action

a. PA Coordinator. CNRSW will appoint a PA Coordinator for the Region. A sample appointing order is attached as enclosure (2). The PA Coordinator will be the principal Point of Contact (POC) for all PA matters within NRSW. The PA Coordinator will inform CNO (DNS-36) when a new Navy PA system of records notice is needed, or when a system of records notice needs to be amended/altered or is no longer necessary. The PA Coordinator will ensure compliance with reference (a) throughout CNRSW's Area of Responsibility (AOR). It is the PA Coordinator's responsibility to disseminate updates and changes to PA protocols. These changes may be found at http://www.privacy.navy.mil. The PA Coordinator will also

monitor the annual list of all systems of record notices submitted by the Installation Commanding Officer (ICO) and Program Director (PD) PA POCs. The PA Coordinator is responsible for the annual review and update of this instruction.

b. PA Team. A PA Team will be appointed to identify procedures to ensure there is no inadvertent release of PPI and to establish best PA business practices within NRSW. The PA Team will oversee and direct commands/programs PA POCs to conduct self-assessments of their commands/programs PA practices and take necessary corrective actions. See enclosure 3 for PA self-assessment checklist. The PA Team will also review any complaints and reports of noncompliance with the PA.

c. Installation Command/Program Director PA POC. All ICOs and PDs shall appoint, in writing, a PA POC and ensure they are properly trained. See enclosure (2) for sample appointing letter. The appointing letter will be forwarded to the PA Coordinator to ensure a current listing of all PA POCs at all installation commands and programs within CNRSW AOR. The PA POC serves as the principal POC on all PA matters for the command/program and is responsible for effective implementation and compliance with this instruction and reference (a). PA POCs shall submit a list of all systems of records notices used by the command/program to the PA Coordinator not later than 1 October every year.

d. DON Employees/Contractors. DON employees/contractors will comply with subsection 7(i) of reference (a) to safeguard the PA rights of others.

e. Privacy Impact Assessment (PIA). In accordance with reference (a), a PIA will be conducted by IT, or a systems manager, or PA POC, before developing or procuring a general support system or major application that collects, maintains, or disseminates Information in Identifiable Form (IIF) from or about Department of the Navy civilian or military personnel. IIF is information in an IT system or online collection that directly identifies an individual (e.g., name, address, social security number, or other identifying code, telephone number, email address, etc.), or when an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification that may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)

f. Disposition of PA records. PA request files, PA amendment case files, PA accounting of disclosed files, PA control files, PA report files, and PA general administrative files shall be disposed of and destroyed under the time limits and guidance contained in as required by reference (b). Dispose of records from systems of records to prevent inadvertent disclosure. To this end:

(1) Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) Region activities may recycle PA data. Such recycling must be accomplished to ensure that PPI is not compromised. Accordingly, the transfer of large volumes of records in bulk to an authorized disposal activity is not considered a disclosure of records. Any compromise of PPI will be reported in accordance with paragraph 3h of this instruction.

(3) When disposing of or destroying large quantities of records from a system of records, Region activities must ensure that the records are disposed of to preclude easy identification of specific records.

g. PA Request Processing Procedures. The PA Coordinator and command/program PA POCs will process requests for access or copies of PA records in accordance with reference (a). When processing a PA request, the PA Coordinator and PA POC are directed to paragraphs 10 and 13 of reference (a) for further guidance and information.

h. Unauthorized Disclosure Accounting and Reporting. In the event of unauthorized disclosure of PPI, the PA POC will take all the required actions under paragraph 18e of reference (a) and, in addition, will make an immediate report to the PA Coordinator.

4. CNRSW PA Training Program. To meet the PA training requirements outlined in reference (a), all installation commands and programs shall ensure their personnel complete PA training, as follows:

a. Orientation training. Training that provides individuals with a basic understanding of the requirements of the PA as it applies to the individual's job performance. The training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

b. Specialized training. Training that provides information as to the application of specific provisions of this instruction and reference (a) to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this instruction. DOD requires that public affairs officials receive annual training.

c. Management training. Training that provides managers with important information that they should take into account when making management decisions regarding the PA program.

d. PA systems of records training. All ICOs and PDs shall ensure all individuals who work with a PA system of records are trained on the provisions of the PA systems of records notice, this instruction, and reference (a). Training will emphasize individual rights and responsibilities under this instruction and reference (a). The PA Coordinator and all PA POCs must be aware that all the Navy's PA systems of records notices are to be listed at http://www.privacy.navy.mil.

e. Online Training. Online training can be accomplished by accessing this site: http://www.privacy.navy.mil/. Training materials can also be downloaded from this site.

5. Annual Self-Assessment Checklist and Compliance with the PA. The PA Coordinator, PA Team, and PA POCs are directed to review the checklist contained in enclosure (3) annually, or as often as directed by the PA Coordinator, to ensure commands and programs are in compliance with reference (a) and this instruction.

L. R. HERING

Distribution:
Electronic only, via CNRSW Directive website
http://www.cnrsw.navy.mil/admin/index.htm

PRIVACY ACT TERMS AND DEFINITIONS

a. Access. Review or copying a record or parts thereof contained in a system of records by any individual.

b. Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review),to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

c. 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 an individual. Members of the United States Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional group[s, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

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

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

f. Official Use. Within the context of this instruction, this term is used when COMNAVREG Southwest 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.

g. 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, marital status, race, salary, home/office phone numbers, etc.

h. Privacy Act (PA) Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

i. Privacy Act Team (PA Team). An interdisciplinary group composed of the PA Coordinator, a representative (preferably a system manager) from Legal (Office of the General Counsel or Staff Judge Advocate), Information Technology, Human Resources Office, Public Affairs Office, Force Protection, Business Office, Community Support Services, Manpower for civilian and military personnel, and Administrative Department. The PA Team is responsible for overall management and guidance to ensure best Regional PA business practices to safeguard protected personal information from unauthorized disclosure.

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

k. Protected Personal Information (PPI). Any information or characteristics that may be used to distinguish or trace an individual's identity, such as his/her name, social security number, or biometric records.

l. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc), about an individual that is maintained by a COMNAVREG Southwest 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 assigned to the individual, such as a finger or voice print or a photograph.

m. "Routine Use" Disclosure. A disclosure of a record made outside DOD for a purpose that is compatible with the purpose for which the record was collected and maintained by DOD. The "routine use" must have been included in the notice for the system of records published in the Federal Register.

n. Statistical Record. A record maintained only for statistical research, or reporting purposes, and not used in whole or in part in making any determination about a specific individual.

o. System Manager. An official who has overall responsibility for a system of records. He/she may serve at any level in DON. Systems mangers are indicated in the published record systems notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity.)

p. System of Records. A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all PA systems of records must be published in the Federal Register and are also available for viewing or downloading from the Navy's Privacy Act Online web site at http://www.privacy.navy.mil.

COMNAVREGSWINST 5211.1
N05H
24 JUL 2006

S A M P L E

5211
Ser _____/

From: Commander, Navy Region Southwest
To: [Name of Appointed Individual]

Subj: APPOINTMENT AS PRIVACY ACT COORDINATOR

Ref: (a) SECNAVINST 5211.5E
(b) COMNAVREGSWINST 5211.1

1. Per references (a) and (b), effective this date you are appointed as the Privacy Act Coordinator for Commander, Navy Region Southwest.

2. Please familiarize yourself with references (a) and (b) regarding your specific duties and responsibilities.

L. R. HERING

Enclosure (2)

S A M P L E

5211
Ser _____/

From: Commanding Officer/Program Director [command/program]
To: [Name of Appointed Individual]

Subj: APPOINTMENT AS PRIVACY ACT POINT OF CONTACT FOR [COMMAND NAME/FUNCTIONAL PROGRAM]

Ref: (a) SECNAVINST 5211.5E
(b) COMNAVREGSWINST 5211.1

1. Per references (a) and (b), effective this date you are appointed as the Privacy Act Coordinator for Commander, Navy Region Southwest.

2. Please familiarize yourself with references (a) and (b) regarding your specific duties and responsibilities.

[Name of CO/PD]

Copy to:
NRSW PA Coordinator

Checklist for PA Best Practices

Region PA Coordinator/PA Team

Has CNIC provided PA guidance, and has the guidance been implemented within the Region's PA program?

Have all systems of records with applicable system notices been reported to the PA Coordinator by PA POCs?

Have all system of records managers been identified and reported to PA Coordinator by PA POCs?

Are any contractors maintaining or operating a system of records?

Have all personnel been properly trained and is the training documented by a completion certificate or other means?

Have PA POCs reported completion of Privacy 101, 102 and 103 training to the PA Coordinator? (Training located at www.privacy.navy.mil (training))

Have PA POCs identified members of their staff who need to know Privacy 101, 102 and 103? Have those staff members participated in the training? Is their training documented?

Has PA Coordinator reviewed SECNAVINST 5211.5E and Privacy 101, 102 and 103?

Have all personnel been trained on what to do if there is an unauthorized disclosure of PPI? (Report to PA Coordinator)

Does PA Coordinator have established protocol for what to do if an unauthorized disclosure occurs? (Take action to prohibit further disclosure, notify all affected individuals by letter within 10 days which recommends visiting http://www.consumer.gov/idtheft for further guidance, email CNO (DNS-36) a synopsis of the disclosure, number of individuals affected, actions to be taken. Subject line of email should be "Identity Theft Notification".)

Have all PA systems of records notices been published in the Federal Register?

Is a log maintained of all PA releases? (OPNAV Form 5211/9)

Is a disclosure accounting form maintained for unauthorized releases?

Has the staff been properly trained on the collection, storage, use and disposal of PPI?

Work with PAO and/or IT to ensure no PPI is placed on public web sites or public folders.

Conduct annual review of PA systems of records to ensure they are necessary, accurate and complete.

Conduct annual program evaluations of commands and programs to ensure compliance with PA. Use the self-assessment evaluation form at www.privacy.navy.mil (administrative tools) as well as this checklist.

Review and validate PIAs annually for information systems and submit the validation to PA Coordinator for further submission to CNO (DNS-36) for Navy information systems.

When requesting someone provides PPI, is the correct PA statement contained on the document requesting the PPI?

Is there a media campaign (PAO) or information dissemination to highlight awareness of the PA and the obligation to protect personal information from unauthorized release?

Ensure all personnel that work with PPI are aware of this checklist for PA best practices.

Installation Command and Program PA POCs

Regularly inspect recycle bins, ensure no PPI in recycling collection bags.

Has PA POC identified all systems of records within his/her command or program? Does he/she know which systems of records contain PPI? Has he/she reported all systems of records to the PA Coordinator?

Are all personnel who work with the PA systems of records trained on the system notice?

What PA training has taken place within the command and has the training been documented by certificate or other means?

Ensure all relevant personnel, including system of records managers, have completed the web-based Privacy Act 101, 102 and 103 courses?

Is all email correspondence, originating from the command, that contains PPI marked For Official Use Only (FOUO)?

Are all documents containing PPI disposed of via shredder/burn bags or other appropriate method?

Review files to ensure any retrieved by name/personal identifier have a system of records notice. Findings should be reported to the PA Coordinator.

Ensure staff is trained in the proper collection, storage, use and disposition of privacy sensitive material and safeguarding PPI.

Review office protocols to avoid loss of PPI.

Work with PAO and/or IT to ensure PPI is not placed on public web sites or in public folders.

Conduct annual review of PA systems of records to ensure they are necessary, accurate and complete. Report findings to the PA Coordinator.

Do all documents containing PPI have the correct PA statement?

Are all unauthorized system of records reported to the PA Coordinator?

Are all unauthorized disclosures reported to the PA Coordinator?

Are all documents marked before distributed/emailed/faxed to ensure recipient is aware of any PA requirements attached to the document?

Review how information is stored/transmitted on laptops/blackberries/recall rosters and social rosters.