



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

5720

IN REPLY REFER TO

Ser N09B30/1U512446

19 Jan 01

From: Chief of Naval Operations

To: Distribution List

Subj: PRIVACY ACT (PA) POLICY ISSUES

Ref: (a) SECNAVINST 5211.5D

Encl: (1) Procedures for Processing a Routine Use Disclosure for an
Incident Complaint Report (ICR)

1. Please be advised of the following changes regarding the DON's Privacy Act Program:

a. As a result of reorganization, the DON's PA/FOIA Policy Branch has a new code, Chief of Naval Operations (N09B10) vice N09B30. Our address, phone numbers and e-mail addresses remain the same.

b. This confirms prior e-mail notification that the Annual Privacy Act (PA) Report is cancelled. Please advise your constituency of this cancellation. It will be reflected in the revision to reference (a).

c. The Navy has altered PA systems notice N05580-1, Security Incident System, formerly numbered as N05527-1. This will dramatically change how naval activities process requests for Incident Complaint Reports (ICRs). See enclosure (1) for a detailed analysis of how to process a routine use disclosure for access to Navy ICRs.

2. With the movement from a paper-based agency to a computerized one, the use of e-mails and faxes to communicate and transmit personal information, etc., privacy must be addressed if we are to avoid potential lawsuits for unauthorized collection, maintenance and/or disclosure of personal information. It is therefore prudent for you to take the following steps to build a stronger PA program:

a. Ensure that all individuals who interact with privacy data are properly trained (i.e., advised of the need to protect information from unauthorized disclosure, etc).

b. Ensure that you identify a PA systems notice that allows your activity to maintain, collect, and disseminate personal information.

c. Ensure routine use disclosures are annotated on disclosure accounting forms.

d. Interact with your information technology and records management personnel. It is important before databases are created and funds expended for their creation that privacy issues are addressed (i.e., Do we have a PA system of records that covers the collection of information?). The same holds true for forms that directly solicit personal information,

directives that address personal information, etc. In the case of forms that solicit personal information directly from the individual, a Privacy Act Statement must appear on the form. In the case of transmitting personal data, we highly recommend that a statement be placed on the document as follows: "FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE." You may even choose to add on websites where information is accessed by password, the following additional notice "Any misuse or unauthorized release of personal information could result in both civil and criminal penalties."

d. Take time to review our privacy web site at privacy.navy.mil. If this is a daily site you visit, "refresh" your linkage so that all changes to PA systems and the site are reflected. We change approximately 10-20% of our records annually. The section marked "List of Changes Made to the Navy's Privacy Act Systems of Records Notices" provides a quick look at changes made to systems (i.e., additions, amendments, alterations, deletions, and number changes).

e. Ensure that contractor personnel who work with privacy-protected information in their official capacity are properly trained and adhere to DON PA policies contained in reference (a).

f. Work with your web master to ensure that privacy data is not placed on the Internet for viewing by all. Rather, if it is placed on the Internet access should be by password and appropriate warnings added to discourage misuse or unauthorized disclosure of information. Any privacy data placed on the Intranet should also be appropriately marked and warnings shown.

g. Take proactive steps to eliminate unnecessary Privacy Act complaints.

3. Training for 2001

a. Privacy Act training is downloadable from privacy.navy.mil. We highly recommend that you download the PA Brief Sheet along with a copy of those PA systems you routinely use (i.e., umbrella systems such as N05000-1, N05000-2, N05000-3, etc) and provide copies to individuals who maintain such records.

b. There are both government and non-government entities that offer PA training. On the Government side, courses are offered by the Department of Justice and Graduate School, U.S. Department of Agriculture. On the non-governmental side, in March 2001 the American Society of Access Professionals will offer both PA and FOIA training at their Western Regional Conference in Albuquerque, New Mexico.

c. We will also be offering training to activities in the Norfolk, Pensacola, and Jacksonville areas in 2001. Ms. Tracy Ross of my staff is currently working with officials to schedule this training. More information will be disseminated to those areas once dates and training sites are firmed up. Other sites requiring training should let their needs be known to Ms. Ross for future offerings. Any activity wishing to pay for Ms. Ross to conduct specialized Privacy and/or FOIA training should also make their desires known to me.

d. The DOJ book, Freedom of Information Act Guide and Privacy Act Overview is also a wonderful training tool. If you do not have a May 2000 edition and need one, please fax your requirement to this office at (202) 685-6580, Attn: Cassandra Bennett. Limited copies are available. This is now issued every two years, the next one being issued in 2002.

4. Privacy Act issues/questions: This staff is available to answer your questions. You can call us at (202) 685-6545/46 or email us at navyfoia@hq.navy.mil.


DORIS M. LAMA

By direction
(202) 685-6545/DSN 325-6545

USCINCPAC (J0421)	JAG (Code 13)
USCINCFJCOM (J02P)	JAG (Code 14)
ASN (M&RA)	MSC [Code FOIA]
HROC	NAVAUDSVCHQ
S/HHRO	NAVINGEN (Code OOL1)
CMC (Code ARAD)	NAVPGSCOL (Code 006)
CINCUSNAVEUR (Code 0132)	NAVOBSY (Code AS)
CINCLANTFLT (Code N02P6)	NAVSTKAIRWARCEN FALLON NV
COMNAVAIRLANT (Code N02P)	NAVWARCOL (Code 009)
COMNAVSUBLANT (Code N02L1)	NCIS (Code 00JF)
COMNAVSURFLANT (Code N02P)	NCPB (Code 0031)
CINCPACFLT (Code 00J1)	NDW (Code N007)
COMNAVAIRPAC (Code N01J)	OGC (Mr. Fredman)
COMNAVSUBPAC (Code 00J)	ONI (Code OCB3)
COMNAVSURFPAC (Code N00J)	SSP (SP-104)
BCNR	USNA (Code 1E)
BUMED (Code 00L1)	COMNAVMETOCCOM (Code 01L)
CNET (Code OOJE)	COMNAVPERSCOM (Pers-06)
CNR (Code OCCC)	COMNAVREG NE
COMNAVAIRSYSCOM (Code 7.7.6)	COMNAVREG MIDLANT
COMNAVCOMTELCOM (Code N14)	COMNAVREG SE
COMNAVCRUITCOM (Code 017)	COMNAVREG NW
COMNAVFACENCOM (Code OOC)	COMNAVREG SW
COMNAVSEASYSYSCOM (Code 09T3)	COMNAVREG HI
COMNAVSECGRU (Code N00J)	COMNAVRESFOR (Code 003)
COMNAVSPACECOM (Code N171)	COMNAVRESPERSCEN
COMSPECWARCOM (Code 004)	COMNAVSATFECEN (Code 03)
COMNAVSUPSYSCOM (Code 939A)	
COMSPAWARSYSCOM (Code 00C)	

PROCEDURES FOR PROCESSING A ROUTINE USE DISCLOSURE FOR AN
INCIDENT COMPLAINT REPORT (ICR)

1. On January 8, 2001, PA systems notice N05527-1, Security Incident System, which governs the collection, maintenance and dissemination of Incident Complaint Reports (ICRs) was altered. A copy is attached.

a. The number assigned to the systems notice was changed from N05527-1 to N05580-1 to comply with a numbering change to the Standard Subject Identification Code (SSIC).

b. Of greater importance, a routine use disclosure was added that provides base security offices with a mechanism to make a disclosure "To individuals involved in base incidents, their insurance companies, and/or attorneys for the purpose of adjudicating a claim, such as personal injury, traffic accident, or other damage to property" under the provisions of the Privacy Act.

c. While this routine use disclosure does not mean that the entire ICR is releasable, it does permit the release of information needed to adjudicate a claim.

2. This alteration changes the procedures for processing ICRs. Accordingly, recommend the following protocols be established:

a. Apprise the individual, his/her attorney, and/or insurance carrier that they will have access to more information if they submit a written request citing the routine use provision for the systems notice rather than citing the Privacy Act or Freedom of Information Act.

b. Release information that complies with the routine use provision (i.e., release information to the individual, his/her attorney, and/or insurance carrier that is needed to adjudicate the claim. For example, release the names of the individuals involved, insurance company names and policy numbers, home addresses and telephone numbers, tag numbers of vehicles, vehicle registration information, and synopsis of accident/incident.)

c. Do not use 10 U.S.C. 130b, a (b)(3) statute under the provisions of the FOIA, as a basis to withhold information on individuals who are routinely deployable, overseas, or in a sensitive unit. This is not applicable to a routine disclosure under the Privacy Act.

d. Do not assume that the entire ICR is releasable. Those portions determined not to be releasable should be "blanked out." Because this is a routine use disclosure under the Privacy Act, do not cite an exemption to cover the withholding of information, do not provide appeal rights, and do not forward the request to your initial denial authority for signature. Rather, routine use disclosures are signed by the Privacy Act systems manager at the local level.

e. Prior to making the disclosure, fill out a Disclosure Accounting Form (OPNAV 5211/10 which is downloadable from privacy.navy.mil). [Note: The disclosure accounting is required to be kept for 5 years or the life of the record, whichever is later]. A copy of OPNAV 5211/10 is attached.

f. Ensure you file a copy of the request, response letter, and information provided in the case file to reflect what information was disclosed and the basis for the disclosure.

3. If you receive a request from a foreign national who does not have access rights under the provisions of the Privacy Act or someone other than the individuals listed in the routine use paragraph of this systems notice, you must process their requests under the provisions of the FOIA.

4. This change does not affect the Marine Corps since they have their own PA systems notice MMN00018, Base Security Incident Report System, which covers the processing of Incident Complaint Reports for organizational elements of the U.S. Marine Corps. Further, their notice already contains an established routine use that allows disclosure to "individuals in support of insurance claims and civil litigation involving base incidents." Accordingly, they will continue to follow their established release procedures.