



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

5211 IN REPLY REFER TO  
Ser N09B10/2U512894  
22 Mar 02

From: Chief of Naval Operations  
To: Distribution List  
  
Subj: PRIVACY ACT (PA) POLICY ISSUES  
  
Ref: (a) SECNAVINST 5211.5D

1. Please ensure distribution of this policy memo. It will be posted on the Navy's PA On-line Web Site at [privacy.navy.mil/](http://privacy.navy.mil/).
2. Just a reminder, all Navy Privacy Act systems of records are downloadable from our web site at [privacy.navy.mil](http://privacy.navy.mil/). You can also download Marine Corps, DoD and its components, and Government-wide systems from this site. As systems are added, deleted, altered, or amended the site is updated to reflect those changes. Systems managers are responsible for ensuring that CNO (N09B10) is apprised of any changes.
3. As a result of recent inquiries and the incidents of September 11, there is a concerted effort to ensure that our personnel can be contacted. Many activities are involved in updating and/or creating Recall/Social Rosters. The following information is provided to assist you:

a. Recall/Social Rosters

(1) The collection of personal information to formulate or update a Recall/Social Roster is permitted under the Navy's Privacy Act systems notice N05000-3, Organizational Locator and Social Roster.

(2) When directly soliciting personal information from an individual, activities are reminded of the need to include a Privacy Act Statement (PAS) whether the solicitation is done in writing or electronically. A sample PAS for use in requesting information for a recall/social roster is as follows:

Authority: 5 U.S.C. 301, Departmental Regulations and E.O. 9397 (SSN).

Purpose: To notify personnel of office closings; locate personnel and/or next of kin in case of emergency; invite personnel to social functions; recall personnel as necessary.

Routine Uses: Information is close-hold and shared with only those with a need-to-know. Supervisory personnel will have access to information concerning their employees. Administrative/web personnel will have access for purposes of maintaining the data base. Disclosure of information is treated as "For Official Use Only - Privacy Sensitive."

Disclosure: Mandatory for military. Mandatory for civilian employees who have been designated by their organization as "emergency personnel." Voluntary for all others. However, failure to provide information may result in them or their family not being accounted for or contacted during an emergency, invited to a social gathering, etc.

(3) Once the list is compiled, it should be marked "For Official Use Only - Privacy Sensitive - Any misuse or unauthorized disclosure may result in civil and criminal penalties."

(4) Dissemination of this list and access to all or part of the list is driven by an official need-to-know. In many cases, activities will limit access to those individuals who need to have access to specific information, rather than the entire recall roster. For example, the Commanding Officer and Executive Officer may require access to the entire roster, while a Division Director may only require access to information on individuals under his/her division.

(5) When is collection mandatory? Collection is mandatory if the agency is able to impose a penalty on the individual for failing to provide the information. For example, it is mandatory for members of the military because it is a lawful order. Failure to comply with a lawful order may result in disciplinary action being taken.

(6) Posting your recall roster on an Intranet web site: The document must be properly marked and access to all or part of the document should be limited to those officials having an official need-to-know. An effective tool is password access.

b. Collecting and posting photographs of individuals on an Intranet site:

(1) Some activities collect and maintain photographs of their employees. For example, public works centers maintain photographs of their personnel since they do not report to a regular office location and must be identified in case of emergency. Security offices maintain photographs of individuals who are issued badges.

(2) Activities are reminded, however, that while collection of photographs may be permissible, safeguards must be in place to ensure that only those individuals with an official need-to-know have access. There is a clear distinction between need-to-know and want-to-know. Need-to-know is defined as official requirement in line with why the information is being collected.

c. Processing requests that cite the Privacy Act

(1) When a person cites to the Privacy Act in a request, the activity's response letter must address whether or not the request is being processed under the provisions of the Privacy Act. For example, "Your request is not being processed under the provisions of the Privacy Act since the information you seek is not contained in a Privacy Act systems of records notice which is retrieved by your name and personal identifier. Hence, your request is being processed under the provisions of the Freedom of Information Act." Or, "Your request is being denied under the provisions of the Privacy Act under exemption \_\_\_\_\_. Accordingly, your request is being processed under the provisions of the Freedom of Information Act."

(2) When processing any request, activities must review all documents associated with the request. For example, if you are reviewing an investigation that lists enclosures, the enclosures must be processed unless the requester has asked for only the basic investigation.

(3) In compliance with Department of Justice reporting requirements, all Privacy Act requests must be counted as Freedom of Information Act requests.

d. The DOJ book, Freedom of Information Act Guide and Privacy Act Overview is being revised and is expected to be received by July. This publication is issued every other year. If you need a copy, please fax your requirement to this office at (202) 685-6580, Attn: Cassandra Bennett. Limited copies of the Case List will also be available.

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

Distribution:

USCINCPAC (J1411)	COMNAVREG NW
USCINCFCOM (J024)	COMNAVREG SW
ASN (M&RA)	COMNAVREG HI
HROC	COMNAVRESFOR (Code 003)
S/HHRO	COMNAVRESPERSCEN
CMC (Code ARAD)	COMNAVSAFECEN (Code 03)
CINCUSNAVEUR (Code 0132)	COMNAVSEASYSYSCOM (Code 09T3)
CINCLANTFLT (Code N02P6)	COMNAVSECGRU (Code N00J)
COMNAVAIRLANT (Code N02L)	COMNAVSPACECOM (Code N171)
COMNAVSUBLANT (Code N02L1)	COMSPECWARCOM (Code 004)
COMNAVSURFLANT (Code N02L)	COMNAVSUPSYSCOM (Code 939A)
CINCPACFLT (Code N00JPL)	COMSPAWARSYSCOM (Code 00C)
COMNAVAIRPAC (Code N01J)	JAG (Code 13)
COMNAVSUBPAC (Code 00J)	JAG (Code 14)
COMNAVSURFPAC (Code N00J)	MSC [Code N9(FOIA)]
BCNR	NAVAUDSVCHQ
BUMED (Code 00L1)	NAVINSGEN (Code OOL1)
CNET (Code OOJE)	NAVPGSCOL (Code 006)
CNR (Code OOC)	NAVOBSY (Code AS)
COMNAVAIRSYSCOM (Code 7.7.6)	NAVSTKAIRWARCEN FALLON NV
COMNAVCRUITCOM (Code 017)	NAVWARCOL (Code 009)
COMNAVFACENCOM (Code OOC)	NCIS (Code 00JF)
COMNAVMETOCOM (Code 01L)	NCPB (Code 0031)
COMNAVNETOPSCEN (Code 014A)	NDW (Code N007)
COMNAVPERSCOM (Pers-06)	OGC (Mr. Fredman)
COMNAVREG NE	ONI (Code OCB3)
COMNAVREG MIDLANT	SSP (SP-104)
COMNAVREG SE	USNA (Code 1E)