



UNITED STATES MARINE CORPS

LEGAL SERVICE SUPPORT TEAM
POSTAL SERVICE CENTER 8007
CHERRY POINT, NORTH CAROLINA 28533-5001

IN REPLY REFER TO:

5800

PAC

NOV 08 2012

From: Privacy Act Coordinator, MCAS Cherry Point
To: All Privacy Act Systems of Records Managers

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

Ref: (a) 5 U.S.C. § 552a (Privacy Act of 1974)
(b) SECNAVINST 5211.5E
(c) SECNAV M-5210.1
(d) ALNAV 059/06
(e) ALNAV 070/07
(f) ECSD Directive 011
(g) MCIEASTO 5211.1B

Encl: (1) Disclosure Accounting Form (OPNAV 5211/9)
(2) Record of Disclosure/Consent Authorization
(3) General Purpose Privacy Act Statement (OPNAV 5211/12)
(4) Loss or Compromise of Personally Identifiable Information (PII) (OPNAV5211/13)

1. In accordance with references (a)-(g), I have issued this memorandum in order to provide notice and training regarding your roles and responsibilities as the Privacy Act System of Records Manager for your respective commands.

2. Overview of the Privacy Act. The Privacy Act of 1974 (reference (a)), establishes safeguards for the protection of records the Government collects and maintains on United States citizens or lawfully admitted permanent residents. Specifically, it mandates that the Government:

a. Inform people at the time it is collecting information about them, why this information is being collected, and how it will be used;

b. Publish a notice in the Federal Register of new or revised systems of records on individuals;

c. Publish a notice in the Federal Register before conducting computer matching programs;

d. Assure that the information is accurate, relevant, timely, and complete before disclosing it to others;

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

- e. Allow individuals access to records on themselves;
- f. Allow individuals to find out about disclosures of their records to other agencies or persons; and
- g. Provide individuals with the opportunity to correct inaccuracies in their records.

3. Privacy Rights. Individuals have the right to seek access to records about themselves; to know to whom records have been disclosed; to request amendment of erroneous information (factual not opinion); and to seek redress in the courts if denied access or amendment.

4. Background to Privacy Act

a. A Privacy Act (PA) System of Records Notice (SORN) is a "blueprint" which delineates the kinds of information that naval activities may collect, maintain, and disseminate on individuals. Department of Defense and Government-wide System of Records Notices are listed on the Defense Privacy and Civil Liberties Office website: <http://dpclo.defense.gov/privacy/SORNS/SORNS.html>

b. Each systems notice is assigned a six-digit number that is preceded by the letter "N" for Navy, "M" for Marine Corps, "NM" for both. The number is based on the Standard Subject Identification Code (SSIC), preceded by "0" for 4 digit SSIC number (i.e., N05300-1).

c. The systems notice provides the keeper of the system and the subject of the system with specific information on what may be contained in the system. More specifically, it identifies the kind of information being collected and on whom, the authority for collecting the information, where it is located, how it is filed, to whom it is routinely disclosed, instructions on how to access the information contained in the system, how long it will be maintained and where the information was obtained.

d. The kinds of systems we maintain are:

(1) Umbrella systems. These are generic systems of records that anyone in the Navy is eligible to use. To identify an umbrella system, look under the section of the systems notice entitled "LOCATION," and it will state "Organizational elements of the Department of the Navy." Examples of commonly used "umbrella" systems are NM05000-1, General Correspondence Files and NM05000-2, Program Management and Locator System (This system covers areas such as recall and social rosters).

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

(2) Limited-use system. These are systems which are approved for use by specific Navy activities. To identify such systems, look under the section of the systems notice entitled "LOCATION."

(3) Exempt systems. These are systems that exempt certain kinds of information from disclosure to the requester. To determine if a system is exempt, look at the last entry in the PA systems notice that reads "Exemptions Claimed for the System," and it will identify what exemptions are being claimed for the system.

(4) Non-exempt systems. These are systems that are releasable to the subject of the file in their entirety. Look at the last entry in the PA systems notice that reads "Exemptions Claimed for the System" and it will state "None."

5. Initial Responsibilities. As a PA Systems Manager, you are assigned duties which include the collection, use, and maintenance of personal information maintained in a PA systems of records notice. It is imperative that you understand the Privacy Act and your role and responsibilities as a systems manager. In the beginning, you will want to:

a. Get to know Ms. Lisa Good, the Command's PA Coordinator (252) 466-6871 and Mr. David Morey, the Command's PA Officer (252) 466-5575; and

b. Obtain and review the following documents:

(1) SECNAVINST 5211.5E, Department of the Navy Privacy Act (PA) Program; and

(2) SECNAV M-5210.1 Department of the Navy Records Management Program; and

(3) ALNAV 059/06 Safeguarding Personal Information; and

(4) ALNAV 070/07 DoN Personally Identifiable Information;
and

(5) Marine Corps Enterprise Cybersecurity Directive 011 (ECSD 011); and

(6) Marine Corps Installations East Privacy Act Instruction (MCIEASTO 5211.1B); and

c. Receive training on the provisions of the Privacy Act (<http://www.doncio.navy.mil/ContentView.aspx?ID=905>); and

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

d. Review the PA systems notice that you have responsibility for to ensure that you are collecting, maintaining, and disseminating information in accordance with the systems notice, and if you identify any discrepancies or need to amend, alter, or delete the system from the Navy's inventory, promptly contact your Command PA Coordinator or CNO (DNS-36) for assistance.

6. Your Role and Responsibility as a Privacy Act Systems of Records Manager

a. **A PA Systems Manager is an individual who is responsible for establishing and maintaining records that are retrieved by a name or other personal identifier that are contained in a PA systems of records notice.**

b. PA Systems of Records Managers are responsible for:

(1) Establishing operational rules and procedures to ensure that anyone who has access to records in a PA system of records fully understands both the safeguarding and maintenance requirements to be followed.

(2) Responding to PA requests for viewing and amendment by acknowledging receipt of a PA request or amendment request within 10 working days and provide a substantive response within 30 days;

(3) Coordinating denial of a PA request or request for amendment with your denial authority, and issuing denial decisions normally within 30 days of receipt;

(4) Ensuring that the command maintains no unpublished systems of records, meaning that no system of records retrieved by a personal identifier is maintained without prior public notice in the Federal Register;

(5) Advising and seeking guidance from the command Privacy Act Coordinator whenever they need to establish, amend, alter, or delete a systems of record notice;

(6) Ensuring that no information is disclosed from any record within your system without the specific written consent of the record subject, unless such disclosure is otherwise permitted by statute;

(7) Obtaining reasonable verification of identity when an individual seeks to access his or her information in a PA system of records (military ID, driver's license, CAC card, etc.);

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

(8) Ensuring that all records maintained in your system of records contain information that is accurate, timely, and complete;

(9) Establishing appropriate administrative, technical, and physical safeguards to ensure security and confidentiality of records and information maintained in your system of records;

(10) Ensuring that all disclosure requests are properly processed according to paragraph 13 of reference (b) and paragraph (13) of reference (f);

(11) Complying with all rules established by the PA systems notice and PA instructions, requiring that you:

(a) must review the PA systems notice annually to determine if the system's maintenance is still required and if so, if it requires changes (pen and ink changes can be submitted to CNO (DNS-36) via FAX (202) 685-6580 or DSN 325-6580 for assistance);

(b) may not collect any new categories of records unless an alteration to the PA systems notice is approved and the changes to the systems notice have been approved and published in the Federal Register;

(c) only release information from the PA systems notice to an organization listed as a "Routine User" in the systems notice and only if the release is consistent with the reason listed in the systems notice (i.e., to the Department of Labor for support of compensation claim);

(d) only release information contained in a PA systems of records notice to Department of Defense/Navy employees who have a "need-to-know," consistent with the "purpose" listed in the systems notice;

(e) must keep and maintain a disclosure accounting form that reflects all releases made of the record to any "routine user" of the system (refer to enclosure (1) for example Disclosure Accounting Form);

(f) must provide guidance and courteous assistance to any individual who requests an opportunity to review, copy, or correct allegedly incorrect information about themselves contained in the system in accordance with the procedures described in paragraph 11 of reference (b) and paragraph (8) of reference (g);

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

(g) must ensure that when you solicit personal information directly from the individual that they are provided a Privacy Act Statement that complies with the PA systems notice (i.e., same authority, purpose, etc.) Refer to Enclosure(4);

(h) must train your personnel on their responsibilities regarding the collection, use, and maintenance of the information contained in the PA systems notice;

(i) must ensure that records maintained in the PA system of records notice are retained for the period specified in the systems notice and that retention period is the same as that contained in the records disposal manual, SECNAV M-5210.1 (reference (c)); and

(j) must ensure that employees are responsible for assuring that personal information they receive as part of their official duties is kept private and that employees who handle records adhere to rules of conduct to protect information from the possibility of unwarranted disclosure or access by unauthorized persons (examples of personal information include an individual's home address, home telephone number, social security number, date and place of birth, etc.)

(12) Ensuring that all command officials

(a) collect personal information only when it is necessary to accomplish an agency purpose that is mandated by statute or executive order;

(b) are aware that portions of information in certain PA systems of records may be exempt from PA disclosure;

(c) are aware that the Secretary of the Navy and/or his delegated representatives are the only officials authorized to adopt rules designating eligible DON system of records as exempt from certain PA requirements;

(d) are aware the information concerning an exempt system must be published in the Federal Register;

(e) are aware that only the head of the command or his designated official(s) may deny access to information maintained in an exempt system of records falling under his cognizance;

(f) ensure that full or truncated SSNs are not included as part of any printed personnel reports, rosters, award certificates, correspondence, or local forms, that if they are used, that they comply with the provisions in reference (f);

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

(g) ensure that password protections are in place for electronic sites and folders maintained on network shared files in accord with section 5 of reference (f);

(h) ensure that personal privacy information is never posted on any command publicly accessible website in accord with section 5 of reference (f);

(i) ensure that all documents containing personal privacy information are appropriately marked as "FOR OFFICIAL USE ONLY" (FOUO);

(j) ensure that all documents containing personal privacy information are appropriately shredded when retention and/or maintenance is no longer required;

(k) ensure that command personnel encrypt all e-mail containing personal privacy information using PKI authentication via the Common Access Card;

(l) ensure that command personnel encrypt, password protect, and transport using secure file transfer protocol (FTP) or Virtual Private Network (VPN) whenever electronic data files require the electronic transfer from one system to another or across the NMCI network;

(m) ensure that command personnel never store personal privacy data on a removable storage device such as CD-ROM, floppy disk, thumb drive, DVD, or laptop computer unless the data is encrypted and password protected and that no PII is placed on personal computers or devices;

(n) ensure that all personnel tasked with transporting records containing personal privacy information transport that data in a manner that prevents disclosure of the contents; and

(o) ensure that appropriate cover sheets are applied to all transported documents containing personal privacy information.

(p) ensure that documents containing personal privacy information are not placed unprotected in guard mail envelopes.

7. Warnings

a. DO NOT

(1) collect personal information without determining that you have an authorized need for the information; or

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

- (2) file personal information in such a way that it can be retrieved by an individual's name, social security number, or other personal identifier, unless you have identified a PA systems of records notice that permits such collection.

b. DO When soliciting information directly from an individual, ensure they are provided a Privacy Act Statement (refer to Enclosure 3) that advises them of the following:

- (1) Authority: what authorizes collection of this information? Refer to the PA systems notice that applies and ensure that when soliciting the social security number, you cite Executive Order (EO) 9397 and the additional law or statute that allows for the collection of the social security number. Ensure forms containing the social security number meet one of the 12 acceptable uses provided in reference (f). In any case, you may not require the social security number if the systems notice does not authorize collection.

- (2) Purpose: specify why the information is being requested. The "purpose" is listed in the systems notice.

- (3) Routine Uses: identify who will routinely have access to this information and for what purpose. The "routine use" is listed in the systems notice.

- (4) Voluntary or Mandatory: in most cases the request for such information is voluntary, unless a specific law or statute requires the information. Normally, you can state that the "information requested is voluntary; however, failure to provide such information may result in _____."

8. Disclosure Accounting. The Privacy Act requires an accounting of disclosure of information from records pertaining to United States citizens and lawfully admitted permanent residents except for disclosure within DOD/DON, or disclosures made under the Freedom of Information Act. The Disclosure Accounting record must contain the date, nature, and purpose of the disclosure, and the name and address of the person or agency to whom disclosure was made. A copy of another agency's request and your reply furnishing the information requested are recommended for the necessary accounting for disclosures made without the consent of the record subject. These accounting records must be placed in the files from which disclosures have been made. Refer to enclosures (1) and (2).

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

9. Criminal Penalties. If you commit one of the following violations, you can be charged with a misdemeanor and fined not more than \$5,000 (per instance):

- a. Willfully disclosing individually identifiable information to any person or agency not entitled to receive it.

- (1) Maintain records that can be retrieved by an individual's name, social security number, payroll number or any other personal identifier unless a notice has been published in the Federal Register.

- (2) Knowingly and willfully obtain any record concerning an individual from an agency under false pretenses.

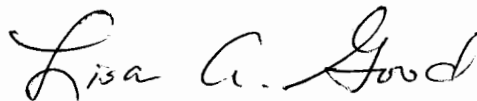
10. Civil penalties. An individual may bring a civil action against your agency in the district courts of the United States for violations of the Privacy Act. If the court determines that your agency acted in a manner that was intentional or willful, the United States can be liable in an amount equal to the sum of the actual damages sustained by the individual, but not less than \$1,000, and the costs of the suit together with reasonable attorney fees.

11. Breach Reporting. 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 references (b) and (f) utilizing the Department of Navy (DoN) Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form at Enclosure (4).

12. Summary. It is essential that each PA Systems Manager is aware of his/her responsibilities under the Privacy Act to protect the security of personal information; to ensure its accuracy, relevance, timeliness, and completeness; to avoid unauthorized disclosures either orally or in writing; and to ensure that no system or records retrieved by personal identifier is maintained without prior public notice in the Federal Register. Through increased awareness among PA System Managers of the importance of safeguarding Privacy Act information and supporting Freedom of Information Act (FOIA)/Privacy Act (PA) program objectives, the DON can effectively balance openness with protection of individual privacy and remain responsive to the public's interest in Government.

Subj: RESPONSIBILITIES OF A PRIVACY ACT SYSTEM OF RECORDS MANAGER

12. The Point of Contact for this matter is Lisa Good, MCAS
Cherry Point Freedom of Information Act/Privacy Act Coordinator,
at (252) 466-6871.

A handwritten signature in cursive script that reads "Lisa A. Good". The signature is written in black ink and is positioned to the right of the typed name.

LISA A. GOOD

RECORD OF DISCLOSURE/CONSENT AUTHORIZATION

1. Identifying Information on Subject

- a. Name of Individual: _____
- b. Grade: _____
- c. Social Security Number: _____

2. Pertinent Data to Whom Disclosure was Made

- a. Date of Disclosure: _____
- b. Nature and Purpose of Disclosure:

- c. Name of Person to Whom Disclosure Made:

- d. Address and Phone Number of Person to Whom Disclosure Made:

- e. Office to Which Disclosure was Made:

3. Information on Person Making Disclosure

- a. Name: _____
- b. Grade: _____
- c. Office or Title: _____
- d. Duty Station Address: _____

"I hereby authorize the Marine Corps to verify my SSN or other identifier and disclose my _____ to officials so that they may contact me in connection with my financial business with _____. All information furnished will be used solely in connection with my financial business relationship with _____."

Signature of Individual

GENERAL PURPOSE PRIVACY ACT STATEMENT

PART A - IDENTIFICATION OF REQUIREMENT

- | | |
|--|-----------------|
| 1. REQUIRING DOCUMENT (Describe - SECNAVINST, OPNAVNOTE, SECNAV ltr, etc.) | 2. SPONSOR CODE |
| 3. DESCRIPTIVE TITLE OR REQUIREMENT (Form title, report title, etc.) | |

PART B - INFORMATION TO BE FURNISHED TO INDIVIDUAL

- | |
|---|
| 1. AUTHORITY |
| 2. PRINCIPLE PURPOSE(S) |
| 3. ROUTINE USE(S) |
| 4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION |

PART C - IDENTIFICATION OF FORM/REPORT/OTHER REQUIREMENT

- | | |
|---|-----------------------|
| 1. FORM NO./REPORT CONTROL SYMBOL/ OTHER IDENTIFICATION | PRIVACY ACT STATEMENT |
|---|-----------------------|

DEPARTMENT OF THE NAVY (DON)
LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)
BREACH REPORTING FORM

This form is intended to provide information regarding the INITIAL REPORT of a loss or suspected loss of PII (i.e., a breach). As additional breach information becomes available, this form can be submitted as often as necessary as a SUPPLEMENTAL REPORT. Select the report type from the drop down menu above. **DO NOT DELAY** submission due to lack of information.

US-CERT Number: _____
(In most cases, the US-CERT number will not be available for inclusion in the initial report. Please provide in supplemental report, when available.)

Today's Date: _____

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:
5. Component (<i>BUMED Activities should Select CNO</i>):	
6. Organization/Branch/Unit Office:	

LOSS OF PII/BREACH INFORMATION

7. Date of Breach: _____ 8. Breach Discovery Date: _____ 9. Breach Discovery Time: _____
(The one hour reporting requirement to notify US-CERT begins at the Date and Time command became aware of the breach. Use military format for time (i.e. 0930, 1455))

10. Individuals Affected by Breach:

Government Civilians: _____	Government Contractors: _____	Military (Active): _____
Military (Reserve): _____	Military (Dependent): _____	Military (Retired): _____
Members of the Public: _____	Other: _____	If Other, Specify: _____
Total Number of Individuals Affected by Breach:		0

11. Type of PII Lost (e.g., SSNs, Financial Data, Medical Data, etc):

12. Brief Description of the breach. Do not include specific names or PII of personnel whose information was lost or compromised.

DATA STORAGE/COLLECTION MEDIA TYPE INFORMATION

13. Data Storage/Collection/Media Type involved in Breach:	14. If Other or More Than One Type, Specify:	
15. If the Breach Involved Hardware or Equipment, was the equipment (Check All That Apply):		
<input type="checkbox"/> Personally Owned	<input type="checkbox"/> Government Owned	<input type="checkbox"/> Contractor Owned
<input type="checkbox"/> Encrypted	<input type="checkbox"/> Password Protected	<input type="checkbox"/> PK Enabled
16. If the Breach involved a Government Credit Card, was the Issuing Bank Notified: <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
17. What was the Cause of the Breach?		
18. If Other, Specify:		

ORGANIZATION DESIGNATED OFFICIAL

19. Name:	20. Title:
21. Phone Number:	22. E-mail Address:

Individual Notifications:

Based on information provided in this report, a risk analysis will be conducted by the DON CIO Privacy Office. If the analysis leads to the determination of a high risk potential for identity theft, this report's Organization Designated Official will be contacted within 24 hours and provided with additional guidance regarding the requirement for notifying individuals.

SENIOR OFFICIAL SIGNING NOTIFICATION LETTERS (IF APPLICABLE) (Usually the Commanding Officer)

23. Name:	24. Title:
25. Phone Number:	26. E-mail Address:

Submit Initial Report for SECNAV/NAVY Breaches

Submit Initial Report for MARINE CORPS Breaches

Submit Initial Report for BUMED Breaches

Submit Supplemental Report for SECNAV/NAVY Breaches

Submit Supplemental Report for MARINE CORPS Breaches

Submit Supplemental Report for BUMED Breaches

If this form will not work with your version of Adobe Acrobat, please follow the procedure in DON CIO WASHINGTON DC 291652Z FEB 08 LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS or MARINE CORPS ENTERPRISE INFORMATION ASSURANCE DIRECTIVE 011