DEPARTMENT OF THE NAVY
NAVY EXCHANGE SERVICE COMMAND
3280 VIRGINIA BEACH BOULEVARD
VIRGINIA BEACH, VA 23452-5724

IN REPLY REFER TO:

NEXCOMINST 5510.1
OC:DS
FEB 3 2010

NEXCOM INSTRUCTION 5510.1

From: Commander, Navy Exchange Service Command

Subj: NOTIFICATION PROCEDURES FOR BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Ref: (a) DoDD 5400.11, 8 May 2007, DoD Privacy Program
(b) DoDD 5400.11-R, 14 May 2007, Department of Defense Privacy Program
(c) OMB Memo M-07-16, 22 May 2007, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
(d) OSD (DA&M) Memo, 21 Sep 2007, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
(e) eGovernment Act of 2002, Title III, Federal Information Security Management Act 2002
(f) NEXCOM Instruction 5211.1, Privacy Act Program
(g) DON CIO Message: Dtg: 291652Z Feb 08, Loss of Personally Identifiable Information (PII) Reporting Process

Encl: (1) NEXCOM Reporting Process for Known or Suspected Loss or Breach of Personally Identifiable Information (PII)
(2) NEXCOM Breach Reporting Form for Initial Loss or Compromise of Personally Identifiable Information (PII)
(3) NEXCOM After Breach Action Reporting Form for Loss or Compromise of Personally Identifiable Information (PII)

1. Purpose. In compliance with references (a) through (e), this instruction establishes the process and requirements for incident reporting when there is a known or suspected loss or breach of Navy Exchange Service Command (NEXCOM) personally identifiable information (PII). Establishment and implementation of this instruction is intended to promote privacy and security awareness and PII handling compliance.

2. Policy. Reference (f) provides NEXCOM's privacy guidelines that are designed to protect the individual privacy of all associates. All Navy Exchange System (NES) associates will strictly adhere to the requirements and procedures provided in enclosures (1) and (2) when responding to a breach, or suspected breach, of PII.

3. Scope. This instruction applies to all NES associates, military and civilian, including Navy Lodge associates, Navy Clothing and Textile Research Facility (NCTRF) personnel, as well as all NES contracted personnel. All NES personnel and contractors must be aware of this instruction and adhere to the process and procedures for identifying and reporting a known breach, or suspected loss, of PII to their supervisor and/or manager.

4. Background. In accordance with reference (g), this instruction incorporates current guidance and reporting process for a breach or loss of PII. The measures contained herein are intended to reduce the risk of identity theft for our Sailors, Marines, their dependents, NES civilian employees, and NES contractor personnel. For the purpose of this instruction, definitions for the terms PII and breach are as follows:

a. PII refers to information which can be used to distinguish or trace an individual's identity, e.g., name, social security number, date and place of birth, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, mother's maiden name, biometric, personal medical and/or financial information, and other demographic data, including any other personal information which is linked or linkable to a specific individual.

b. Breach is the term used to describe the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for other than authorized purposes, have access or potential access to physical or electronic PII, or any suspected occurrence of any of the above situations.

5. Responsibility

a. Headquarters: The Single Digit Codes (SDCs) are responsible for ensuring that procedures are adhered to by all NES associates and contractor personnel. Enclosure (1) provides the reporting process when there is a known or suspected breach of PII. Completion of enclosure (2) is required for reporting any initial loss or compromise of PII. SDCs will complete, and/or accept, review and submit as appropriate for action. Additionally, SDCs are responsible for the subsequent follow-up action required for completion of enclosure (3).

b. Field Activities: District Vice Presidents (DVPs) are to oversee the program for all Navy Exchanges (NEXs) under their purview and provide guidance as required. DVPs, General Managers (GMs) and Branch Exchange Managers (BEMs) are responsible for ensuring that procedures are adhered to by all NES associates and contractor personnel. Navy Lodge Regional Managers (NLRMs) are to oversee the program for all Navy Lodges under their purview and provide guidance as required. NLRMs and Navy Lodge Managers are responsible for ensuring that procedures are adhered to by all associates and contractor personnel. Enclosure (1) provides the reporting process when there is a known or suspected breach of PII. Completion of enclosure (2) is required for reporting any initial loss or compromise of PII. DVPs, GMs and BEMs will complete, and/or accept, review and submit as appropriate for action. Additionally, DVPs, GMs and BEMs are responsible for the subsequent follow-up action required for completion of enclosure (3).

c. NES Associates. All NES personnel, military and civilian, as well as contracted personnel are responsible for adhering to the policy as established in this instruction.

6. Action. This instruction is effective immediately. Addressees will:

a. Take immediate action to ensure widest dissemination to all NES associates and contractors.

b. Implement the policies, procedures, and actions required for safeguarding and reporting PII breaches as stated herein.

c. Maintain records, completed forms, and training certificates for periodic audits/inspections at each activity.

d. Designate a representative to act as the department/activity point of contact (POC) responsible for chain of command coordination to ensure reporting of PII breaches and follow-up actions.

POC for guidance or questions associated with implementation of this instruction is Office of Counsel, Code OC, Office Manager and FOIA Program Coordinator, at (757) 631-3613.

MICHAEL P. GOOD
Executive Vice President
Chief Operating Officer

Distribution:
NEXCOMINST 5218.1
List 1 (Office Staff/Directors/Staff Assistants & Direct Reports)
List A (District Vice Presidents)
List C (GMs NEXs)
List D (NEXMARTs)
List F (Navy Lodge Managers/DoD Reservation Center)
District Loss Prevention/Safety Managers
Distribution Center Loss Prevention/Safety Managers
Regional Logistic Managers
Navy Clothing and Textile Research Facility

Copy:
COMNAVSUPSYSCOM

Stocked:
Electronic only via NEXCOM web site https://nexweb.nexnet.navy.mil/

**NEXCOM REPORTING PROCESS
FOR KNOWN OR SUSPECTED LOSS OR BREACH OF
PERSONALLY IDENTIFIABLE INFORMATION (PII)**

The reporting process when there is a known or suspected loss or breach of Navy Exchange Service Command (NEXCOM) PII is as follows:

1. All NEXCOM personnel (i.e., military, civilian, Navy Lodge, NCTRF, and contractors) will be responsible to report a known breach or suspected breach or loss of PII to their immediate supervisor. Enclosure (2) will be completed by the reporting person's immediate supervisor, manager, GM, BEM, DVP, NLRM, or Navy Lodge Manager and forwarded via email to their appropriate department head/director (i.e, Single Digit Code) and the FOIA/PA Coordinator at donna_l._simpson@nexweb.org. Enclosure (2) should be as complete as possible, to include the following information, but shall not be delayed due to lack of detailed information.

a. Component/organization involved;

b. Date of incident, the number of individuals impacted, and whether they are government, civilian, military, and/or private citizens (include percentage of each category);

c. Brief description of incident, including circumstances of the breach, type of information lost or compromised, and if the PII was encrypted or password protected.

2. The FOIA/PA Coordinator will be responsible to ensure Department of Defense (DoD) and Federal Information Security Management Act (FISMA) reporting requirements are met as well as notifying and coordinating appropriate headquarters departmental personnel to ensure necessary actions are taken to resolve the reported PII breach.

3. Upon resolution of the initial breach report, the FOIA/PA Coordinator will ensure the originator of the initial report completes enclosure (3) and is subsequently distributed to appropriate NEXCOM departments, personnel, and in accordance with DoD directives and FISMA requirements.

NEXCOM BREACH REPORTING FORM
FOR
INITIAL LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

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. **DO NOT DELAY** submission due to lack of information.

Today's Date:_____

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:
5. Activity:	
6. Organization/Branch/Activity No.	

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. Number of Individuals Affected by Breach:

Government Civilians: _____ Government Contractors:_____ Military (Active):_____

Military (Reserve): _____ Military Dependant: _____ Military (Retired):_____

Members of the Public:_____ Other: _____ If Other, Specify: _____

Total Number of Individuals Affected by Breach: _____

11. Type of PII Loss (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):

Personally Owned _____ Government Owned _____ Contractor Owned _____

Encrypted _____ Password Protected _____ PK Enabled _____

16. If the Breach involved a Government Credit Card, was the issuing bank notified? ____ Yes ____ No ____ N/A

17. What was the cause of the Breach?

18. If Other, Specify

NEXCOM AFTER BREACH ACTION REPORTING FORM FOR LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

This form is intended to provide additional breach information and the status of follow-up actions as information becomes available. It may be used multiple times, as required.	
Today's Date: _____	
Person Making Initial Report	
1. Name	2. Title
3. Phone Number	4. Email Address:
5. Activity	
6. Organization/Breach/Activity No	
Additional Breach Information and Status of Follow-up Actions	
7. Provide actions taken to prevent reoccurrence:	
8. Provide lessons learned.	
9. If breach occurred on a IT system, provide system name:	10. If a paper document or e-mail, was it marked correctly? _____Yes _____No _____N/A