DON CIO MESSAGE: DTG: 291652Z FEB 08

UNCLASSIFIED//

SUBJ/LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS//

REF/A/MSG/DON CIO WASHINGTON DC/301540ZNOV2006//
REF/B/DOC/DOD/21SEP2007// REF/C/MSG/SECNAV/042232ZOCT2007//
REF/D/MSG/DON CIO WASHINGTON DC/171952ZAPR2007//

NARR/REF A IS DEPARTMENT OF THE NAVY (DON) LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS. REF B IS DEPARTMENT OF DEFENSE (DOD) GUIDANCE ON SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PII. REF C IS DON PII ANNUAL TRAINING POLICY. REF D IS DON INTERIM POLICY FOR HANDLING PII ON PORTABLE ELECTRONIC DEVICES//

POC/STEVE MUCK/CIVPERS/DON CIO/LOC: WASHINGTON DC/TEL: 703-602-4412/EMAIL: STEVEN.MUCK@NAVY.MIL//

POC/DORIS LAMA/CIVPERS/DNS-36/LOC: WASHINGTON DC/TEL: 202-685-6545/EMAIL: DORIS.LAMA@NAVY.MIL//

PASSING INSTRUCTIONS:
CNO - PLEASE PASS TO DNS/N091/N093/N095/N097/N1/N2/N3/N5/N4/N6/N8//

NAVY ECHELON 1 AND 2 COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER /N1/N6//AND PRIVACY OFFICERS//

USMC MAJOR SUBORDINATE COMMANDS: PLEASE PASS TO G1/G6 AND PRIVACY OFFICERS//

1. PURPOSE. THIS MESSAGE ANNOUNCES THE UPDATED REPORTING PROCESS TO BE USED WHEN THERE IS A KNOWN OR SUSPECTED LOSS OF DEPARTMENT OF THE NAVY (DON) PERSONALLY IDENTIFIABLE INFORMATION (PII). IT INCLUDES NEW AND EXISTING REQUIREMENTS FOR INCIDENT REPORTING RECENTLY ISSUED BY THE OFFICE OF MANAGEMENT AND BUDGET (OMB) AND THE DEPARTMENT OF DEFENSE (DOD).

2. SCOPE. ALL DON PERSONNEL (I.E., MILITARY, CIVILIAN, AND CONTRACTORS) MUST BE AWARE OF THEIR ROLES AND RESPONSIBILITIES RELATED TO REPORTING A KNOWN OR SUSPECTED LOSS OF PII. DON PERSONNEL WHO HAVE DISCOVERED A KNOWN OR SUSPECTED LOSS OF PII MUST REPORT THE BREACH TO THEIR SUPERVISOR. COMMANDS/ACTIVITIES WILL DESIGNATE AN OFFICIAL IN THE CHAIN OF COMMAND RESPONSIBLE FOR REPORTING PII BREACHES AND TO SERVE AS A POINT OF CONTACT (POC) FOR FOLLOW-UP ACTIONS AND INDIVIDUAL NOTIFICATIONS.

3. BACKGROUND. THIS MESSAGE CANCELS AND SUPERSEDES THE REPORTING PROCESS DESCRIBED IN REF A. IT INCORPORATES THE LATEST GUIDANCE REGARDING THE DEFINITION OF PII AND THE REPORTING PROCESS FOR THE LOSS OF PII IDENTIFIED IN REF B. REF C WAS IMPLEMENTED TO PROMOTE PRIVACY AND SECURITY AWARENESS AND PII HANDLING COMPLIANCE. THESE MEASURES, ALONG WITH THE INSTRUCTIONS IN REF D FOR HANDLING PII ON PORTABLE ELECTRONIC DEVICES, ARE INTENDED TO REDUCE THE RISK OF IDENTITY THEFT TO OUR SAILORS, MARINES, THEIR DEPENDENTS, CIVILIAN PERSONNEL AND CONTRACTOR PERSONNEL.

4. PER REF B, 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, PERSONNEL, MEDICAL, FINANCIAL INFORMATION, AND OTHER DEMOGRAPHIC DATA, INCLUDING ANY OTHER PERSONAL INFORMATION WHICH IS LINKED OR LINKABLE TO A SPECIFIED INDIVIDUAL.

5. PER REF B, THE TERM ?BREACH? IS USED TO INCLUDE 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 PURPOSE, HAVE ACCESS OR POTENTIAL ACCESS TO PII, WHETHER PHYSICAL OR ELECTRONIC.

6. ACTION. THE UPDATED PROCESS OUTLINED BELOW WILL BE USED FOR REPORTING A KNOWN OR SUSPECTED LOSS OF PII. THE DESIGNATED OFFICIAL OF THE ACCOUNTABLE COMMAND/ACTIVITY WILL:

A. WITHIN ONE HOUR OF THE DISCOVERY OF A LOSS OR SUSPECTED LOSS OF PII, NOTIFY VIA A SINGLE EMAIL THE FOLLOWING PRIVACY OFFICIALS AND AGENCIES OF THE LOSS:

(1) ADDRESS TO: THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT), SOC@US-CERT.GOV.

(2) COPY TO: DON CIO PRIVACY TEAM, DON.PRIVACY.FCT@NAVY.MIL; DOD PRIVACY OFFICE, DOD.PRIVACY@OSD.MIL AND PIA@OSD.MIL; THE CHIEF OF INFORMATION (CHINFO), CHINFO.DUTYOFFIC.FCT@NAVY.MIL.

(3) IN ADDITION, FOR USMC BREACHES, INCLUDE AS COPY TO: THE MARINE CORPS PRIVACY ACT OFFICER, SMBHQMCPRIVACYACT@USMC.MIL AND THE USMC HQ C4 INFORMATION ASSURANCE (IA) BRANCH, HQMC_C4IA_IDMGT@USMC.MIL.

B. THE EMAIL SHOULD INCLUDE THE FOLLOWING INFORMATION, BUT SHALL NOT BE DELAYED DUE TO LACK OF DETAILED INFORMATION:

(1) COMPONENT/ORGANIZATION INVOLVED;

(2) DATE OF INCIDENT, THE NUMBER OF INDIVIDUALS IMPACTED, AND WHETHER THEY ARE GOVERNMENT CIVILIAN, MILITARY, AND/OR PRIVATE CITIZENS (INCLUDE PERCENTAGE OF EACH CATEGORY);

(3) BRIEF DESCRIPTION OF INCIDENT, INCLUDING CIRCUMSTANCES OF THE BREACH, TYPE OF INFORMATION LOST OR COMPROMISED, AND IF THE PII WAS ENCRYPTED OR PASSWORD PROTECTED.

C. IF COMMISSION OF A CRIME IS SUSPECTED, NOTIFY THE LOCAL NAVAL CRIMINAL INVESTIGATIVE SERVICE (NAVCRIMINVSERV) OFFICE OR MARINE CORPS CRIMINAL INVESTIGATION DIVISION (CID) TO CONDUCT AN INVESTIGATION.

D. CONTACT THE LOCAL STAFF JUDGE ADVOCATE (SJA) OR OFFICE OF GENERAL COUNCIL (OGC).

E. IF THE BREACH INVOLVED THE LOSS OR SUSPECTED LOSS OF A GOVERNMENT AUTHORIZED CREDIT CARD OR ASSOCIATED FINANCIAL DATA ASSOCIATED WITH THE CARD, IMMEDIATELY NOTIFY THE ISSUING BANK, AND THE COMMAND?S GOVERNEMENT CREDIT CARD MANAGER.

F. WHEN APPLICABLE, ISSUE AN OPREP3, IN ACCORDANCE WITH OPREP3 REPORTING PROCEDURES.

G. WITHIN 24 HOURS AFTER RECEIPT, THE DON CIO PRIVACY OFFICE WILL REVIEW THE INITIAL BREACH REPORT AND DETERMINE, USING DOD?S RISK ANALYSIS METHODOLOGY IN REF B, THE POTENTIAL RISK OF HARM TO IMPACTED PERSONNEL. BASED UPON THIS REVIEW, THE DON CIO PRIVACY OFFICE WILL NOTIFY THE ORGANIZATION?S DESIGNATED OFFICIAL OF THE REQUIRED NOTIFICATIONS, IF ANY.

H. NOTIFICATIONS, IF REQUIRED, ARE TO BE MADE WITHIN TEN (10) DAYS OF THE DISCOVERY OF LOSS OR SUSPECTED LOSS OF PII. THE DESIGNATED OFFICIAL SHALL, BY WRITTEN LETTER OR DIGITALLY SIGNED EMAIL, NOTIFY ALL IMPACTED INDIVIDUALS. A SAMPLE NOTIFICATION LETTER IS AVAILABLE AT HTTP://PRIVACY.NAVY.MIL. IF THE TEN (10) DAY REQUIREMENT IS NOT MET, THE DESIGNATED OFFICIAL MUST NOTIFY THE DON CIO PRIVACY OFFICE, PROVIDE THE REASON WHY NOTIFICATION WAS NOT MADE, AND WHAT ACTIONS ARE BEING TAKEN TO COMPLETE THE NOTIFICATION PROCESS. FOR ALL INCIDENTS THAT REQUIRE NOTIFICATION, THE COMMAND/ACTIVITY IS DIRECTED TO INVESTIGATE WHETHER DON POLICY WAS FOLLOWED. IN CASES WHERE POLICY WAS NOT FOLLOWED, APPROPRIATE DISCIPLINARY ACTION SHOULD BE TAKEN, WEIGHING MITIGATING CIRCUMSTANCES, SEVERITY OF THE PII LOSS OR COMPROMISE, AND OTHER EXTENUATING FACTORS.

I. AS SOON AS ADDITIONAL BREACH INFORMATION BECOMES AVAILABLE THE DESIGNATED OFFICIAL WILL SUBMIT THIS INFORMATION TO THE DON CIO PRIVACY OFFICE VIA EMAIL.

J. WHEN IMPACTED PERSONNEL CANNOT BE LOCATED OR DIRECTLY CONTACTED, THE COMMAND/ACTIVITY SHOULD USE ANY MEANS THAT WILL LIKELY SUCCEED IN REACHING THE IMPACTED INDIVIDUALS, SUCH AS ESTABLISHING A TOLL-FREE NUMBER (I.E., CALL CENTER) IN ACCORDANCE WITH GUIDANCE PROVIDED AT HTTP://PRIVACY.NAVY.MIL (SEE ADMINISTRATIVE TOOLS, GUIDELINES, FOR SETTING UP A CALL CENTER) .

K. THE DESIGNATED OFFICIAL WILL ENSURE THE FOLLOWING INFORMATION IS SENT TO THE DON CIO PRIVACY OFFICE AS SOON AS AVAILABLE, BUT NO LATER THAN 30 DAYS AFTER DISCOVERY OF LOSS OR SUSPECTED LOSS OF PII: REMEDIAL ACTIONS TAKEN TO PREVENT REOCCURRANCE; INDIVIDUAL NOTIFICATION STATUS, IF NOTIFICATIONS WERE REQUIRED; LESSONS LEARNED, IF AVAILABLE; AND DISCIPLINARY ACTION TAKEN, WHERE APPROPRIATE.

7. THE NEW REPORTING PROCEDURES FOR KNOWN OR SUSPECTED PII BREACHES ARE EFFECTIVE IMMEDIATELY AND ARE MANDATORY FOR ALL DON COMMANDS/ACTIVITIES. IN ADDITION, AUTOMATED REPORTING FORMS THAT WILL STREAMLINE AND STANDARDIZE THE REPORTING PROCESS WILL BE FORTHCOMING.

8. AMPLIFYING INFORMATION CAN BE FOUND IN REF B THROUGH REF D AND IS POSTED AT HTTP://PRIVACY.NAVY.MIL. USMC SPECIFIC REQUIREMENTS ARE OUTLINED IN MARADMINS 267/07 AND 447/07 AND POSTED ON HTTPS://HQDOD.HQMC.USMC.MIL/PII.ASP.

9. RELEASED BY ROBERT J. CAREY, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.//