DTG: 171952Z APR 07
SUBJECT: SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

UNCLASSIFIED
MSGID/GENADMIN/DON CIO WASHINGTON DC//

REF/A/DOC/OMB/22MAY2006//
REF/B/DOC/OMB/23JUN2006//
REF/C/DOC/OMB/12JUL2006//
REF/D/DOC/DOD/18AUG2006//
REF/E/DOC/DOD/18AUG2006//
REF/F/DOC/SECNAV/28DEC2005//
REF/G/DOC/DONCIO/30NOV2006//
REF/H/DOC/DOD/06FEB2003//

NARR/REF A IS OMB GUIDANCE M-06-15 ON SAFEGUARDING PII. REF B IS OMB GUIDANCE M-06-16 ON PROTECTING SENSITIVE AGENCY INFORMATION. REF C IS UPDATED OMB GUIDANCE M-06-19 ON REPORTING INCIDENTS INVOLVING PII. REF D IS DOD GUIDANCE ON PROTECTING PII. REF E IS DOD GUIDANCE ON PROTECTING DATA AT REST ON PORTABLE COMPUTING DEVICES. REF F IS SECNAVINST 5211.5E, DEPARTMENT OF THE NAVY (DON) PRIVACY PROGRAM. REF G OUTLINES REPORTING PROCEDURES WHEN A LOSS OF PII OCCURS. REF H IS DODI 8500.2 FOR INFORMATION ASSURANCE IMPLEMENTATION.

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

PASSING INSTRUCTIONS:
CNO: PLEASE PASS TO DNS/N091/N093/N095/N097/N1/N2/N3/N5/N4/N6/N8//
NAVY ECHELON II COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER (IO)/N1/N6//
CMC PLEASE PASS TO DMCS/C4/AR///
USMC FORCE AND USMC SUBORDINATE COMMANDS - PLEASE PASS TO COMMAND INFORMATION OFFICER (IO)/G1/G6//

RMKS/1. PURPOSE. THIS MESSAGE ESTABLISHES INTERIM POLICY FOR THE HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION (PII) WHEN STORED ON GOVERNMENT FURNISHED LAPTOP COMPUTERS, OTHER MOBILE COMPUTING DEVICES AND REMOVABLE STORAGE MEDIA. (E.G., REMOVABLE HARD DRIVES, THUMB DRIVES, BLACKBERRIES, PERSONAL DIGITAL ASSISTANTS (PDAS), COMPACT DISCS, DVDS, ETC.).

2. BACKGROUND. DESPITE CURRENT GUIDANCE PROVIDED IN REFS A THROUGH G, THERE CONTINUES TO BE A NUMBER OF INCIDENTS WHERE PERSONALLY IDENTIFIABLE INFORMATION (PII) HAS BEEN LOST OR STOLEN. MOST OF THESE INCIDENTS CAN BE ATTRIBUTED TO THE CARELESS MISUSE OR LOSS OF LAPTOP COMPUTERS, OTHER MOBILE COMPUTING DEVICES OR REMOVABLE STORAGE MEDIA. THIS UNACCEPTABLE TREND CONTINUES TO HINDER OUR WARFIGHTING ABILITY AT EVERY LEVEL AND KEEPS OUR GREATEST RESOURCE SAILORS AND MARINES - FROM FOCUSING ON THE DAY-TO-DAY ISSUES THE DON IS REQUIRED TO SUPPORT. AS SUCH, SENIOR LEADERSHIP MUST BE ACTIVELY ENGAGED IN REDUCING AND/OR ELIMINATING THE NUMBER OF INCIDENTS OCCURRING WITHIN OUR DEPARTMENT AND HOLDING THOSE RESPONSIBLE FOR THE LOSS ACCOUNTABLE.

3. DISCUSSION. PER REFS C AND D, PII IS ANY INFORMATION ABOUT AN INDIVIDUAL MAINTAINED BY AN AGENCY, INCLUDING, BUT NOT LIMITED TO, EDUCATION, FINANCIAL TRANSACTIONS, MEDICAL HISTORY, AND CRIMINAL OR

EMPLOYMENT HISTORY AND INFORMATION WHICH CAN BE USED TO DISTINGUISH OR TRACE AN INDIVIDUAL S IDENTITY, SUCH AS THEIR NAME, SOCIAL SECURITY NUMBER, DATE AND PLACE OF BIRTH, MOTHER S MAIDEN NAME, BIOMETRIC RECORDS, ETC., INCLUDING ANY OTHER PERSONAL INFORMATION WHICH IS LINKED OR LINKABLE TO AN INDIVIDUAL.

4. ACTION. DON CIO AND DNS-36 ARE CURRENTLY CO-CHAIRING A PII INCIDENT REDUCTION WORKING GROUP TO REVIEW EXISTING POLICY AND PROVIDE NEW GUIDANCE/POLICY AS NECESSARY. A COMPREHENSIVE REVIEW OF PII HANDLING/STORAGE IS UNDERWAY AND NEW POLICY WILL BE FORTHCOMING. AS AN INTERIM MEASURE, DON PERSONNEL ARE DIRECTED TO IMPLEMENT THE FOLLOWING POLICY IMMEDIATELY:

A. PER REF D, ANY LAPTOP COMPUTER, MOBILE COMPUTING DEVICE OR REMOVABLE STORAGE MEDIA THAT PROCESSES OR STORES A COMPILATION OF ELECTRONIC RECORDS CONTAINING PII ON 25 OR MORE INDIVIDUALS ON A SINGLE DEVICE (OR LESS THAN 25 INDIVIDUALS WHERE THE DATA OWNER IDENTIFIES A REQUIREMENT FOR ADDITIONAL PROTECTIVE MEASURES) SHALL BE RESTRICTED TO DOD OWNED, LEASED, OR OCCUPIED WORKPLACES. WHEN COMPELLING OPERATIONAL NEEDS REQUIRE REMOVAL FROM THE WORKPLACE, THE LAPTOP COMPUTER, MOBILE COMPUTING DEVICE OR REMOVABLE STORAGE MEDIA SHALL:

(1) BE SIGNED IN AND OUT WITH A SUPERVISING OFFICIAL DESIGNATED IN WRITING BY SENIOR LEADERSHIP.

(2) BE CONFIGURED TO REQUIRE CERTIFICATE BASED AUTHENTICATION FOR LOG ON (FOR LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES WHERE POSSIBLE).

(3) BE SET TO IMPLEMENT SCREEN LOCK, WITH A SPECIFIED PERIOD OF INACTIVITY NOT TO EXCEED 15 MINUTES (FOR LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES WHERE POSSIBLE).

(4) HAVE ALL PII STORED ON, CREATED ON, OR WRITTEN FROM LAPTOP COMPUTERS, MOBILE COMPUTING DEVICES AND REMOVABLE STORAGE MEDIA AS APPLICABLE ENCRYPTED. (MINIMALLY NIST-CERTIFIED, FIPS 140-2 OR CURRENT) A DOD ENTERPRISE SOLUTION IS BEING DEVELOPED FOR ENCRYPTING ALL STORED DATA. AS AN INTERIM SOLUTION, WINZIP 9.0 AND ABOVE, WHICH IS AVAILABLE ON MOST DESKTOPS, PROVIDES THE REQUIRED ENCRYPTION PROTECTION USING FIPS-197 CERTIFIED ADVANCED ENCRYPTION STANDARD (AES). WINZIP PASSWORDS SHOULD BE AT LEAST NINE CHARACTERS LONG AND CONTAIN THE FOLLOWING: AN UPPER CASE LETTER, A LOWER CASE LETTER, A NUMBER, AND A SPECIAL CHARACTER. PASSWORDS SHOULD NOT HAVE SEQUENTIAL NUMBERS, CONTAIN ANY DICTIONARY WORDS, OR CONTAIN YOUR FIRST OR LAST NAME. WINZIP ENCRYPTED FILES MAY BE STORED ON SYSTEM HARD DISKS OR TRANSFERRED TO EXTERNAL STORAGE MEDIA AS REQUIRED. USERS NEED TO BE AWARE THAT WHEN WINZIP IS USED TO ENCRYPT A FILE, A NEW ENCRYPTED FILE IS CREATED AND THE ORIGINAL FILE REMAINS UNALTERED ON THE RESIDENT DEVICE. IN SOME CASES THIS ORIGINAL UNENCRYPTED FILE SHOULD BE DELETED TO MAINTAIN SECURITY OF THE PII (E.G., WHEN WINZIP IS USED TO ENCRYPT A FILE ON A THUMB DRIVE OR OTHER REMOVABLE STORAGE MEDIA).

B. EFFECTIVE 01 OCTOBER 2007, STORAGE OF ANY FORM OF PII IS PROHIBITED ON PERSONALLY OWNED LAPTOP COMPUTERS, MOBILE COMPUTING DEVICES AND REMOVABLE STORAGE MEDIA.

C. PER REF H, LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES AND THE DATA STORED ON REMOVABLE STORAGE MEDIA MUST BE PASSWORD PROTECTED. PASSWORDS SHOULD BE AT LEAST NINE CHARACTERS LONG AND CONTAIN THE FOLLOWING: AN UPPER CASE LETTER, A LOWER CASE LETTER, A NUMBER, AND A SPECIAL CHARACTER. PASSWORDS SHOULD NOT HAVE SEQUENTIAL NUMBERS, CONTAIN ANY DICTIONARY WORDS, OR CONTAIN YOUR FIRST OR LAST NAME.

D. PER REF F, ENSURE ALL DOCUMENTS CONTAINING PII ARE MARKED FOR OFFICIAL USE ONLY PRIVACY SENSITIVE ANY MISUSE OR UNAUTHORIZED DISCLOSURE CAN RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES. UNDERSTANDING THE IMPACT OF THIS REQUIREMENT ON CERTAIN ORGANIZATIONS, UNTIL DOCUMENTS ARE UPDATED TO CONTAIN THE ABOVE STATEMENT, THEY SHOULD BE AT A MINIMUM STAMPED FOUO PRIVACY SENSITIVE .

E. ENSURE PROMPT AND COMPLETE REPORTING OF ALL PII INCIDENTS AND SUSPECTED INCIDENTS IAW REF G. THIS INCLUDES REPORTING WHETHER THE LOSS REPORTED WAS ENCRYPTED AS REQUIRED ABOVE.

5. THE DON PRIVACY WEB SITE IS AN OFFICIAL SOURCE OF POLICY, GUIDANCE, TRAINING, AND INFORMATION REGARDING THE SAFEGUARDING AND HANDLING OF PII, AND INCIDENT REPORTING REQUIREMENTS. REFERENCES LISTED ABOVE AND THE WINZIP ENCRYPTION PROCESS CAN BE FOUND ON THE DON PRIVACY WEB SITE AT HTTP://PRIVACY.NAVY.MIL.

6. REQUEST WIDEST DISSEMINATION.

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