DON CIO Message DTG: 202041Z AUG 07

UNCLASSIFIED//

SUBJ: DON SECURITY GUIDANCE FOR PERSONAL ELECTRONIC DEVICES (PED)

MSGID/GENADMIN/DON CIO WASHINGTON DC//

REF/A/DOC/DOD/01APR2004//
REF/B/MSG/DON CIO WASHINGTON DC/061525ZOCT2004//
REF/C/DOC/DOD/24OCT2002//
REF/D/MSG/CNO WASHINGTON DC/072022ZDEC2004//
REF/E/MSG/CMC WASHINGTON DC/041820ZMAY2005//

NARR/REF A IS DODINST 8520.2, PUBLIC KEY INFRASTRUCTURE AND PUBLIC KEY ENABLING. REF B IS THE DON CIO PKI IMPLEMENTATION GUIDANCE UPDATE MESSAGE. REF C IS THE DOD INFORMATION ASSURANCE DIRECTIVE 8500.1. REF D IS CNO MESSAGE, COMMON ACCESS CARD (CAC) AND PUBLIC KEY INFRASTRUCTURE. REF E IS MARADMIN 209/05, WHICH PROVIDES USMC GUIDANCE UPDATE ON PEDS.

POC/JAMES MAUCK/CTR/DONCIO/LOC:ARLINGTON, VA/TEL:703-601-0579/E-MAIL: JAMES.MAUCK.CTR@NAVY.MIL/

RMKS/1. POLICY. REF A REQUIRES THAT ALL DEPARTMENT OF DEFENSE (DOD) INFORMATION SYSTEMS, INCLUDING NETWORKS AND E-MAIL SYSTEMS, BE ENABLED TO USE DOD ISSUED PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATES TO SUPPORT AUTHENTICATION, ACCESS CONTROL, CONFIDENTIALITY, DATA INTEGRITY, AND NONREPUDIATION. PER REF B, DEPARTMENT OF THE NAVY (DON) USERS SHALL DIGITALLY SIGN E-MAIL MESSAGES REQUIRING EITHER MESSAGE INTEGRITY AND/OR NON-REPUDIATION, AND ENCRYPT MESSAGES CONTAINING SENSITIVE INFORMATION, DEFINED BY REF C PARA E2.1.41. E-MAIL THAT IS ROUTINE, PERSONAL, OR NON-OFFICIAL IN NATURE (E.G., SAILOR MAIL) SHOULD NOT BE DIGITALLY SIGNED. REFS D AND E PROVIDE SERVICE SPECIFIC GUIDANCE FOR APPROPRIATE USE OF DIGITAL SIGNATURE AND ENCRYPTION OF E-MAIL.

2. TECHNOLOGICAL ADVANCES HAVE ENABLED MORE PERVASIVE USE OF DIGITAL SIGNATURE AND ENCRYPTION OF E-MAIL WITHIN THE DON. USE OF THESE DIGITAL SIGNATURES IS EXPECTED TO INCREASE IN THE PREVENTION OF E-MAIL SPOOFING AND SPEAR-PHISHING ATTACKS. E-MAIL ENCRYPTION IS BEING USED MORE OFTEN AS A MEANS TO PROTECT E-MAIL CONTAINING PERSONALLY IDENTIFIABLE INFORMATION (PII), PRIVACY ACT, AND OTHER CATEGORIES OF DOD SENSITIVE INFORMATION WHILE IN TRANSIT ACROSS DOD NETWORKS. THESE CAPABILITIES MUST BE SUPPORTED ON ALL PERSONAL ELECTRONIC DEVICES (PED) SERVING AS AN EXTENSION OF THE DON ENTERPRISE NETWORK.

3. ALL PEDS MUST BE CAPABLE OF SUPPORTING DIGITAL SIGNATURE AND ENCRYPTION (SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)) FUNCTIONALITY. IN ADDITION, PEDS MUST BE ABLE TO INTERFACE WITH THE PKI CERTIFICATES STORED ON DOD-APPROVED HARDWARE TOKENS INCLUDING THE COMMON ACCESS CARD (CAC). ALL PED INTERCONNECTIONS MUST BE MADE USING A DESIGNATED ACCREDITING AUTHORITY (DAA) APPROVED DEVICE THROUGH EITHER A PHYSICAL CONNECTION OR A SECURED BLUETOOTH COMMUNICATIONS LINK, CONFIGURED IN ACCORDANCE WITH THE DEFENSE INFORMATION SECURITY AGENCY (DISA) WIRELESS SECURITY IMPLEMENTATION GUIDE (STIG). IMPLEMENTATION

OF THESE TWO ENHANCEMENTS IS ESSENTIAL FOR A FULLY PK-ENABLED AND INTEROPERABLE PED SOLUTION FOR MOBILE ACCESS TO DON E-MAIL SERVICES.

4. COMMANDS ARE ENCOURAGED TO IMMEDIATELY BEGIN TRANSITION TO PEDS SUPPORTING DIGITAL SIGNATURE AND ENCRYPTION. EFFECTIVE 31 MARCH 2008, USE OF PEDS WHICH ARE NOT NATIVELY COMPLIANT OR HAVE NOT BEEN UPGRADED TO MEET THE REQUIREMENTS IDENTIFIED IN PARAGRAPH 3 WILL NO LONGER BE PERMITTED. ESTABLISHMENT OF NEW CONTRACTS OR RENEWAL OF OLD CONTRACTS FOR INCOMPATIBLE DEVICES IS PROHIBITED.

5. TO PROTECT PEDS FROM UNAUTHORIZED ACCESS AND FEATURES THAT POSE POTENTIAL SECURITY VULNERABILITIES, THE DEFAULT SECURITY CONFIGURATION FOR ALL DON PEDS WILL BE UPGRADED IN ACCORDANCE WITH THE DISA WIRELESS STIG AND DAA-APPROVED DEVIATIONS. THE NEW CONFIGURATION WILL BECOME THE DON STANDARD AND MUST BE APPLIED TO ALL PEDS AUTHORIZED FOR USE ON ANY DON NETWORK.

6. FOR THE NMCI ENVIRONMENT, A LIST OF ACCREDITED AND SECURITY COMPLIANT DEVICES CAN BE FOUND ON THE NMCI HOMEPORT AT HTTPS://WWW.HOMEPORT.NAVY.MIL/SERVICES/BLACKBERRY/. FURTHER SERVICE-SPECIFIC AND NMCI IMPLEMENTATION DETAILS WILL BE PROVIDED UNDER SEPARATE COVER.

7. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.

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