

UNCLASSIFIED//

PRECEDENCE TO: ROUTINE DTG: 032009Z OCT 08
PRECEDENCE CC: ROUTINE
TYPE: DMS SIGNED/ENCRYPTED
FROM PLA: DON CIO WASHINGTON DC

ORIGINAL TO RECIPIENTS:

CNO N6
CMC C4
COMUSFLTFORCOM NORFOLK VA//
COMUSNAVEUR NAPLES IT//
COMPACFLT PEARL HARBOR HI//
USNA ANNAPOLIS MD//
COMUSNAVCENT BAHRAIN//
COMNAVRESFORCOM NEW ORLEANS LA//
COMNAVVAIRSYSCOM PATUXENT RIVER MD///
BUMED WASHINGTON DC//
NETC PENSACOLA FL//
COMNAVSEASYSYSCOM WASHINGTON DC//
FLDSUPPACT WASHINGTON DC//
COMNAVVSUPSYSCOM MECHANICSBURG PA//
DIRSSP WASHINGTON DC//
CNIC WASHINGTON DC//
PRESINSURV NORFOLK VA//
COMNAVLEGSVCCOM WASHINGTON DC//
NAVPGSCOL MONTEREY CA//
COMNAVAFACENCOM WASHINGTON DC//
COMNAVSAFECEN NORFOLK VA//
BUPERS MILLINGTON TN//
NAVWARCOL NEWPORT RI//
ONI WASHINGTON DC//
COMNAVSPECWARCOM CORONDAO CA//
COMSPAWARSYSCOM SAN DIEGO CA//
COMNAVDIST WASHINGTON DC//
NAVHISTCEN WASHINGTON DC//
NAVY BAND WASHINGTON DC
COMUSNAVSO
COMMARCORSYSCOM QUANTICO VA//
COMMARFOREUR//
COMMARFORLANT//
COMMARFORPAC//
COMMARFORRES//
COMMARFORSOUTH//
CG MCCDC QUANTICO VA//

ORIGINAL CC RECIPIENTS:

DON CIO WASHINGTON DC//
COMNAVNETWARCOM NORFOLK VA//
COMOPTEVFOR NORFOLK VA
DRPM NMCI ARLINGTON VA

UNCLASSIFIED//

SUBJ: DON POLICY UPDATES FOR PERSONAL ELECTRONIC DEVICES (PED) SECURITY

AND APPLICATION OF EMAIL SIGNATURE AND ENCRYPTION

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/042120ZSEP08//

REF/E/MSG/CMC WASHINGTON DC/091429ZJUN08// REF/F/DOC/JTF-GNO/07APR08//

REF/G/MSG/DON CIO WASHINGTON DC/202041ZAUG07//

NARR/REF A IS DOD INSTRUCTION 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, IMPLEMENTATION OF THE NAVY ELECTRONIC MAIL DIGITAL SIGNATURE POLICY. REF E IS MARADMIN 336/08, WHICH PROVIDES USMC POLICY FOR EMAIL DIGITAL SIGNATURE AND ENCRYPTION. REF F IS JOINT TASK FORCE ? GLOBAL NETWORK OPERATIONS COMMUNICATIONS TASKING ORDER 07-015, PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION, REVISION 1. REF G PROVIDED INITIAL GUIDANCE FOR DON PERSONALLY OWNED ELECTRONIC DEVICES.

POC/SONYA SMITH/CIV/DONCIO/LOC: ARLINGTON, VA/TEL :703-604-7059/EMAIL: SONYA.R.SMITH1@NAVY.MIL/

POC/JAMES MAUCK/CTR/DONCIO/LOC: ARLINGTON, VA/TEL:703-413-4009/EMAIL: JAMES.MAUCK.CTR@NAVY.MIL/

RMKS/1. THIS MESSAGE PROVIDES UPDATES TO THE DEPARTMENT OF THE NAVY (DON) POLICY FOR DIGITAL SIGNATURE AND ENCRYPTION OF EMAIL. IT ALSO PROVIDES UPDATED BUDGET GUIDANCE FOR PROCUREMENT AND USE OF SMART CARD READER TECHNOLOGY TO SUPPORT DIGITAL SIGNATURE AND ENCRYPTION OF EMAIL FROM PERSONAL ELECTRONIC DEVICES.

2. POLICY. REF A REQUIRES THAT ALL DEPARTMENT OF DEFENSE (DOD) INFORMATION SYSTEMS, INCLUDING NETWORKS AND E-MAIL SYSTEMS, BE ENABLED TO USE DOD ISSUED OR APPROVED PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATES TO SUPPORT AUTHENTICATION, ACCESS CONTROL, CONFIDENTIALITY, DATA INTEGRITY, AND NON-REPUDIATION. PER REF B, 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. REFS D AND E PROVIDE ADDITIONAL SERVICE SPECIFIC GUIDANCE FOR APPROPRIATE USE OF DIGITAL SIGNATURE AND ENCRYPTION OF EMAIL.

3. REF F INTRODUCES A NEW REQUIREMENT FOR DIGITAL SIGNATURE OF ALL EMAIL, FROM DESKTOPS OR PEDS, CONTAINING EITHER AN ATTACHMENT (FOR EXAMPLE WORD DOCUMENTS, POWERPOINT BRIEFINGS, EXCEL SPREADSHEETS) OR EMBEDDED "CLICKABLE" ACTIVE CONTENT (FOR EXAMPLE "MAILTO" EMAIL LINKS OR WEB SITE UNIFORM RESOURCE LOCATOR (URL) ADDRESSES). USE OF TECHNICAL CONTROLS TO ENFORCE THE SIGNATURE OF EMAIL BY DEFAULT IS PROHIBITED UNLESS USERS ARE ABLE TO MANUALLY DISABLE THE SIGNATURE FUNCTION ON A PER-MESSAGE BASIS. TRANSMISSION OF EMAIL (I.E. CREATE, FORWARD, REPLY, REPLY ALL) THAT SHOULD BE EITHER SIGNED OR ENCRYPTED WITHOUT APPLYING DIGITAL SIGNATURE OR ENCRYPTION IS PROHIBITED, REGARDLESS OF TECHNICAL LIMITATIONS OF THE DESKTOP OR HANDHELD DEVICE BEING USED.

4. TECHNOLOGICAL ADVANCES HAVE ENABLED MORE PERVASIVE USE OF DIGITAL

SIGNATURE AND ENCRYPTION OF EMAIL WITHIN THE DON. USE OF DIGITAL SIGNATURES IS EXPECTED TO INCREASE AS A TOOL TO REDUCE RISK OF ATTACKS THROUGH USE OF TARGETED FRAUDULENT OR "SPOOFED" EMAILS. EMAIL ENCRYPTION IS BEING USED MORE OFTEN AS A MEANS TO PROTECT EMAIL CONTAINING PERSONALLY IDENTIFIABLE INFORMATION (PII), PRIVACY ACT, AND OTHER CATEGORIES OF DOD SENSITIVE INFORMATION WHILE IN TRANSIT ACROSS THE GLOBAL INFORMATION GRID. THESE CAPABILITIES MUST BE SUPPORTED ON ALL PERSONAL ELECTRONIC DEVICES (PED) SERVING AS AN EXTENSION OF DON ENTERPRISE NETWORKS.

5. PERSONAL ELECTRONIC DEVICES: REF G INTRODUCED THE REQUIREMENT FOR ALL PEDS TO BE CAPABLE OF SUPPORTING DIGITAL SIGNATURE OR ENCRYPTION FUNCTIONALITY AND PROVIDED A TIMELINE FOR UPGRADE OF NON-COMPATIBLE DEVICES. ADDITIONALLY REF A REQUIRES ALL PEDS BE CAPABLE OF INTERFACING WITH THE PKI CERTIFICATES STORED ON A SMART CARD LIKE THE DOD COMMON ACCESS CARD (CAC).

6. THE DEPARTMENT HAS MADE PROGRESS IN UPGRADING NON-COMPLIANT PED HANDHELDS, HOWEVER, A SIGNIFICANT NUMBER OF NON-COMPLIANT HANDHELDS REMAIN IN SERVICE. THE DON CHIEF INFORMATION OFFICER (CIO) HAS EXTENDED THE DEADLINE FROM REF G FOR PED HANDHELD UPGRADES UNTIL 31 DECEMBER 08 TO ALLOW FOR USE OF MID-YEAR AND END-OF-YEAR FUNDING RE-ALLOCATIONS TO REPLACE OUT OF DATE DEVICES. NON-COMPLIANT HANDHELD DEVICES WILL BE DISCONNECTED ON 31 DECEMBER 08. THE SERVICES SHALL SUBMIT A PLAN OF ACTION AND MILESTONES (POA&M) FOR DISCONNECTION OF NON-COMPLIANT DEVICES BY 31 OCTOBER 2008.

7. TO ACHIEVE COMPLIANCE WITH THE DIGITAL SIGNATURE POLICY DISCUSSED IN PARAGRAPH 2, PURCHASE AND INSTALLATION OF A DESIGNATED ACCREDITING AUTHORITY (DAA) APPROVED SMART CARD READER IS REQUIRED FOR ALL PEDS. THE DEADLINE FOR CARD READER PURCHASE AND INSTALLATION IS 31 DECEMBER 09, ALLOWING SEVERAL OPPORTUNITIES FOR SUBMISSION OF EXECUTION AND BUDGET YEAR FUNDING ISSUE PAPERS, IF REQUIRED. APPROVED SMART CARD READERS MAY INTERFACE WITH PED HANDHELDS THROUGH EITHER A PHYSICAL CONNECTION OR A SECURED BLUETOOTH COMMUNICATIONS LINK, CONFIGURED IN ACCORDANCE WITH THE DEFENSE INFORMATION SECURITY AGENCY (DISA) WIRELESS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG). DOD PKI SOFTWARE CERTIFICATES SHALL NOT BE ISSUED OR USED AS AN ALTERNATIVE INTERIM SOLUTION FOR CAC-BASED PKI, OR IN INSTANCES WHERE THE REQUIRED CARD READER HARDWARE HAS NOT BEEN PROCURED OR INSTALLED.

8. COMMANDS ARE ENCOURAGED TO IMMEDIATELY BEGIN TRANSITION TO PEDS SUPPORTING DIGITAL SIGNATURE AND ENCRYPTION. INITIATION OR RENEWAL OF CONTRACTS FOR NON-COMPLIANT DEVICES IS PROHIBITED.

9. THE DON CIO RECOGNIZES THE NEED FOR FISCAL FLEXIBILITY IN PROCURING AND IMPLEMENTING THESE CAPABILITIES. THIS FLEXIBILITY MUST BE BALANCED WITH THE NEED FOR INCREASED NETWORK SECURITY ACHIEVED THROUGH THE IMPLEMENTATION OF THE REFERENCED DOD, JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS, AND DON POLICIES. THEREFORE, EMAIL ENCRYPTION AND DIGITAL SIGNATURE POLICY EXCEPTIONS WILL NOT BE GRANTED DUE TO INSUFFICIENT FUNDING FOR DEVICE AND HARDWARE UPGRADES OR LACK OF PROPERLY CONFIGURED DESKTOPS AND PEDS.

10. A LIST OF ACCREDITED AND SECURITY COMPLIANT DEVICES CAN BE FOUND ON THE NMCI HOMEPORT AT

[HTTPS://WWW.HOMEPORT.NAVY.MIL/SERVICES/MOBILE/BLACKBERRY/](https://www.homeport.navy.mil/services/mobile/blackberry/).

11. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.

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