

DON CIO Message

DTG: 031859Z DEC 08

SUBJ: DEPARTMENT OF NAVY POLICY UPDATES FOR USE OF NIPRNET PUBLIC KEY INFRASTRUCTURE SOFTWARE CERTIFICATES

UNCLASSIFIED//

REF/A/ MSG/DON CIO WASHINGTON DC/122213Z MAY 08// REF/B/ DOC/JTF-GNO/07APR08//

NARR/ REF A ANNOUNCES THE DON CIO PKI SOFTWARE CERTIFICATE MINIMIZATION EFFORT. REF B IS JOINT TASK FORCE ? GLOBAL NETWORK OPERATIONS COMMUNICATIONS TASKING ORDER 07-015, PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION, REVISION 1.

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

JAMES MAUCK/CTR/DONCIO/LOC:ARLINGTON, VA/TEL:703-601-0120/E-MAIL: JAMES.MAUCK.CTR@NAVY.MIL/

RMKS/1. ISSUE - CRYPTOGRAPHIC AUTHENTICATION IS A PILLAR OF DEPARTMENT OF DEFENSE (DOD) NETWORK SECURITY. PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATES, WHOSE KEY PAIRS HAVE BEEN GENERATED AND STORED ON A HARDWARE TOKEN (SUCH AS THE COMMON ACCESS CARD (CAC)), PROVIDE HIGHER LEVELS OF ASSURANCE BECAUSE THE STORED PRIVATE KEYS CANNOT BE EXTRACTED FROM THE TOKEN. PKI SOFTWARE CERTIFICATES ARE INHERENTLY NO LESS SECURE THAN THEIR HARDWARE-BASED EQUIVALENT WHEN IMPLEMENTED CORRECTLY; HOWEVER, WHEN SOFTWARE CERTIFICATES ARE IMPROPERLY STORED, INSTALLED, AND/OR CONFIGURED ON COMPUTERS (E.G. WEB BROWSERS), ADDITIONAL NETWORK VULNERABILITIES MAY BE INTRODUCED. DUE TO IMPROPER HANDLING OF SOFTWARE CERTIFICATES IN THE PAST, INCREASED ATTENTION IS BEING FOCUSED ACROSS THE DEPARTMENT OF THE NAVY (DON) ON MINIMIZING/ELIMINATING THE USE OF PKI SOFTWARE CERTIFICATES ON THE NIPRNET WHERE AN ALTERNATIVE EXISTS.

2. EARLIER THIS YEAR, PER REF A, THE DON CHIEF INFORMATION OFFICER (CIO) CONDUCTED AN IMPACT ASSESSMENT AND DATA CALL TO UNDERSTAND WHERE SOFTWARE CERTIFICATES ARE USED IN OUR UNCLASSIFIED ENVIRONMENTS. THE RESULTING INITIAL POLICY CHANGES BASED ON THIS EFFORT ARE LISTED BELOW. SOFTWARE CERTIFICATE USE CASES PREVIOUSLY IDENTIFIED IN REF A REMAIN UNAFFECTED UNLESS IDENTIFIED IN PARAGRAPH 3 BELOW.

3. POLICY CHANGES:

A. INDIVIDUALS WHO ARE AUTHORIZED A COMMON ACCESS CARD MAY NO LONGER BE ISSUED NIPRNET SOFTWARE CERTIFICATES UNLESS DEEMED A MISSION ESSENTIAL REQUIREMENT AND AUTHORIZED BY THE DON DEPUTY CIO (NAVY OR MARINE CORPS). THE NUMBER OF SOFTWARE CERTIFICATES ISSUED FOR PERSONAL USE, AND A DESCRIPTION OF THE ASSOCIATED MISSION REQUIREMENT WILL BE REPORTED SEMI-ANNUALLY BEGINNING ON 1 JULY 2009 TO THE DON CIO VIA THE DON DEPUTY CIO (NAVY OR MARINE CORPS) USING A REPORTING TEMPLATE TO BE PROVIDED SEPCOR. LACK OF THE APPROPRIATE HARDWARE (CARD READER) AND SOFTWARE (E.G. ACTIVCLIENT MIDDLEWARE) FOR USE OF THE CAC IS NO LONGER A VALID REASON FOR ISSUANCE OF SOFTWARE CERTIFICATES FOR PERSONAL USE. ALL SOFTWARE CERTIFICATES MUST BE ISSUED BY AN AUTHORIZED REGISTRATION AUTHORITY (RA) OR LOCAL REGISTRATION AUTHORITY (LRA) ONLY AFTER RECEIVED APPROVAL FROM THE DON DEPUTY CIO (NAVY OR MARINE CORPS). USE OF THE SOFTWARE CERTIFICATE SELF-SERVICE ISSUANCE PROCESSES BY DON END-

USERS IS PROHIBITED; HOWEVER, THIS SERVICE REMAINS AUTHORIZED FOR USE BY REGISTRATION AUTHORITIES/LOCAL REGISTRATION AUTHORITIES AS REQUIRED TO ISSUE CERTIFICATES ON HARDWARE TOKENS (I.E. ALTERNATE TOKENS).

B. AFLOAT CONTINGENCY PLAN - AFLOAT USERS HAVE BEEN PROVIDED WITH CARD READERS AND MIDDLEWARE AND SHOULD BE USING THEIR CAC FOR ALL PKI FUNCTIONS. ON SHIPS THAT DO NOT HAVE THE ABILITY TO ISSUE OR MAINTAIN THE CAC (I.E. THERE IS NO RAPIDS WORKSTATION ON-BOARD) SOFTWARE CERTIFICATES MAY BE USED AS A CONTINGENCY SHOULD A USER'S CAC BECOME LOST, STOLEN, LOCKED, DAMAGED OR OTHERWISE INOPERABLE. SOFTWARE CERTIFICATES SHALL BE INSTALLED IAW REF B AND THE INSTALLATION PROCEDURES AVAILABLE AT [HTTPS:\(SLASH\)\(SLASH\)INFOSEC.NAVY.MIL/PKI/TRAINING.HTML](https://(SLASH)(SLASH)INFOSEC.NAVY.MIL/PKI/TRAINING.HTML). SOFTWARE CERTIFICATE INSTALLATION P12 AND .PFX FILES MUST BE REMOVED FROM WORKSTATIONS IMMEDIATELY AFTER INSTALLATION IN WEB BROWSERS. SOFTWARE CERTIFICATES ISSUED FOR THIS PURPOSE MUST BE TRACKED AND REVOKED UPON COMPLETION OF CAC MAINTENANCE, CAC REPLACEMENT, OR 30 DAYS AFTER THE END OF THE DEPLOYMENT. SOFTWARE CERTIFICATES ISSUED AND REVOKED AS A RESULT OF AFLOAT CONTINGENCY OPERATIONS SHALL BE REPORTED USING THE SAME PROCESS IDENTIFIED IN PARAGRAPH 3.A.

4. THE JOINT TASK FORCE - GLOBAL NETWORK OPERATIONS (JTF-GNO), IN REF B, HAS PROVIDED SPECIFIC GUIDANCE FOR PROPER HANDLING, INSTALLATION, AND MAINTENANCE OF PKI SOFTWARE CERTIFICATES. REF B IS AVAILABLE AT [HTTPS:\(SLASH\)\(SLASH\)WWW.JTFGNO.MIL](https://(SLASH)(SLASH)WWW.JTFGNO.MIL). MARINE CORPS GUIDANCE CAN BE FOUND AT [HTTPS:\(SLASH\)\(SLASH\)WWW.MCNOSC.USMC.MIL/SERVICES/PKI](https://(SLASH)(SLASH)WWW.MCNOSC.USMC.MIL/SERVICES/PKI).

5. FUTURE POLICY AND GUIDANCE UPDATES RELATED TO SOFTWARE CERTIFICATES WILL BE RELEASED AS ADDITIONAL SOFTWARE CERTIFICATE ALTERNATIVE CAPABILITIES BECOME AVAILABLE.

6. REPORTING REQUIREMENT CONTAINED IN THIS MESSAGE ARE EXEMPT FROM REPORT CONTROL SYMBOLS PER SECNAV M-5214.1.

7. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.

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