

***** UNCLASSIFIED// *****

Subject: NAVY TELECOMMUNICATIONS DIRECTIVE (NTD) 05-10 CRYPTOGRAPHIC LOG-ON (CLO)

Originator: COMNAVNETWARCOM VIRGINIA BEACH VA(UC)

DTG: 051248Z May 10

Precedence: ROUTINE

DAC: General

To: AL ALCOM(UC)

ALCOM

Cc: COMNAVNETWARCOM VIRGINIA BEACH VA(UC)

UNCLASSIFIED//

ALCOM 074/10

MSGID/GENADMIN/NAVNETWARCOM/N3/MAY//

SUBJ/NAVY TELECOMMUNICATIONS DIRECTIVE (NTD) 05-10

CRYPTOGRAPHIC /LOG-ON (CLO)//

REF/A/RMG/COMNAVNETWARCOM NORFOLK VA/171303ZAPR2009//

REF/B/DOC/DODI/01APR2004//

REF/C/DOC/JTF-GNO/07APR2008/-/NOTAL//

REF/D/RMG/COMNAVNETWARCOM NORFOLK VA/161230ZJUN2008//

REF/E/RMG/CNO WASHINGTON DC/292147ZJUN2009//

REF/F/DOC/PEO C4I/01SEP2009

REF/G/RMG/COMNAVNETWARCOM NORFOLK VA/061930ZSEP2006//

NARR/REF A IS NAVY TELECOMMUNICATIONS DIRECTIVE (NTD) 04-09

CRYPTOGRAPHIC LOG-ON (CLO), HEREBY SUPERSEDED. REF B IS DODI 8520.2

PUBLIC KEY INFRASTRUCTURE (PKI) AND PUBLIC KEY (PK) ENABLING. REF C IS

JTF-GNO CTO 07-015 REVISION 1, PUBLIC KEY INFRASTRUCTURE (PKI)

IMPLEMENTATION, PHASE 2. REF D IS NETWARCOM CTO 08-07 PKI

IMPLEMENTATION PHASE TWO. REF E IS NAVADMIN 196/09, ISSUANCE OF LOGICAL

ACCESS CREDENTIALS TO CERTAIN VOLUNTEER PERSONNEL. REF F IS DOD MEDIUM

ASSURANCE PKI US NAVY ALTERNATE TOKEN STANDARD OPERATING PROCEDURES

(CURRENT VERSION AND ASSOCIATED ADDENDUMS). REF G IS NTD 07-06, PUBLIC

KEY INFRASTRUCTURE IMPLEMENTATION PLAN.//

POC/SETH B. GANG/CIV/NETWARCOM/LOC:NORFOLK VA/TEL:757-417-6754 X3/

TEL:DSN 537-6754 X3/EMAIL:[SETH.GANG\(AT\)NAVY.MIL](mailto:SETH.GANG(AT)NAVY.MIL)//

POC/FREDDIE L. BLASER/CIV/UNIT:NETWARCOM/NAME:NORFOLK VA

/TEL:757-417-6798 X2/TEL:DSN 537-6798 X2

/EMAIL:[FREDDIE.BLASER\(AT\)NAVY.MIL](mailto:FREDDIE.BLASER(AT)NAVY.MIL)//

1. PURPOSE: CANCEL REF A. THIS NTD PROVIDES UPDATED POLICY AND GUIDANCE ON THE USE OF CRYPTOGRAPHIC LOG-ON (CLO) FOR IDENTIFICATION AND ACCESS CONTROL FOR ALL UNCLASSIFIED NAVY NETWORKS ATTACHED TO THE NIPRNET.

2. SCOPE AND APPLICABILITY: THIS NTD APPLIES TO ALL NAVY NETWORKS ATTACHED TO THE NIPRNET AND IS EFFECTIVE IMMEDIATELY. THIS INCLUDES THE NAVY AND MARINE CORPS INTRANET (NMCI), OCONUS NAVY ENTERPRISE NETWORK (ONE-NET), INTEGRATED SHIPBOARD NETWORK SYSTEM (ISNS), APPROVED EXCEPTED NETWORKS, LEGACY NETWORKS AND ALL OTHER NAVY NETWORK SYSTEMS OR SUBSYSTEMS AS APPROPRIATE.

3. BACKGROUND: REF B REQUIRES USERS TO AUTHENTICATE THEMSELVES TO A NETWORK USING CERTIFICATES ISSUED BY THE DOD PUBLIC KEY INFRASTRUCTURE (PKI) ON A HARDWARE TOKEN SUCH AS THE COMMON ACCESS CARD (CAC) OR AN EQUIVALENT ASSURANCE LEVEL DOD PKI HARDWARE TOKEN. THE CAC SHALL BE THE PRIMARY TOKEN FOR UNCLASSIFIED NETWORKS. AN ALTERNATE LOGON PKI HARDWARE TOKEN (ALT) ISSUED BY THE DOD PKI IS APPROVED FOR CERTAIN USER AND ACCOUNT TYPES. NAVY COMPLIES WITH HIGHER LEVEL DIRECTION ISSUED BY JOINT TASK FORCE - GLOBAL NETWORK OPERATIONS (JTF-GNO) REGARDING SMARTCARD LOGON (SCL), OTHERWISE KNOWN AS CLO IN THE NAVY. REFS C AND D

REFER. REFS E AND F PROVIDE POLICY AND GUIDANCE THAT EXPAND THE TYPE OF ACCOUNTS THAT CAN RECEIVE A DOD PKI HARDWARE TOKEN, THUS ELIMINATING CERTAIN CLO EXCEPTION CATEGORIES.

4. ACTION: ALL USER AND SYSTEM ACCOUNTS ON NAVY NETWORKS CONNECTED TO THE NIPRNET SHALL REQUIRE CLO IN ACCORDANCE WITH REFS B THROUGH D. CLO SHALL BE REQUIRED FOR BOTH LOCAL (DESKTOP) LOGON AND REMOTE ACCESS (E.G., RAS, OWA, REMOTE ADMINISTRATION, ETC.). CLO EXCEPTIONS WILL BE CAREFULLY MONITORED AND KEPT TO ABSOLUTE MINIMUM. THE ONLY AUTHORIZED EXCEPTIONS TO THE CLO REQUIREMENT WILL BE AS CITED IN PARAGRAPHS 5 AND 6 BELOW.

5. AUTHORIZED CLO EXCEPTIONS FOR USER ACCOUNTS: SOME USER POPULATIONS WILL NOT BE ABLE TO PERFORM CLO DUE TO TECHNICAL OR POLICY LIMITATIONS. BELOW ARE THE THREE AUTHORIZED EXCEPTION CATEGORIES FOR USER ACCOUNTS.

A. WAR FIGHTERS: CLO IS NOT REQUIRED FOR DEPLOYED PERSONNEL WHO ARE NOT COLLOCATED (SAME BASE, STATION OR SHIP) WITH REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM (RAPIDS) WORKSTATIONS TO ISSUE CAC OR DO NOT HAVE THE CAPABILITY TO BE ISSUED AN ALT. THIS INCLUDES MOST SHIPBOARD PERSONNEL, EMBASSY PERSONNEL, PROVISIONAL RECONSTRUCTION TEAMS, FIRST RESPONDERS AND COALITION PARTNER LOCATIONS NOT COLLOCATED WITH RAPIDS WORKSTATIONS. CLO WILL NOT BE POSSIBLE ON AFLOAT PLATFORMS UNTIL RAPIDS, ADNS INCREMENT IIA OR BETTER, AND COMPOSE 3.5 OR GREATER ARE INSTALLED; HOWEVER, ALL OTHER PKI REQUIREMENTS APPLY TO AFLOAT PLATFORMS (E.G., DIGITALLY SIGNING EMAIL, ACCESSING PRIVATE WEB SERVERS, ETC).

B. CAC OR ALT TOKEN INELIGIBLE USERS: CLO IS NOT REQUIRED FOR USERS NOT CURRENTLY AUTHORIZED A CAC, ALT TOKEN OR OTHER DOD APPROVED PKI HARDWARE TOKEN. THIS EXCEPTION CATEGORY IS NOW LIMITED TO ONLY NEWLY HIRED PERSONNEL. NEWLY HIRED PERSONNEL ARE NOT REQUIRED TO PERFORM CLO UNTIL THEY ARE ELIGIBLE TO RECEIVE A CAC OR OTHER DOD PKI TOKEN. ALL OTHER PREVIOUSLY CAC INELIGIBLE USERS ARE NOW ELIGIBLE FOR A LOGICAL ACCESS CREDENTIAL OR ALT TOKEN PER REFS E AND F.

C. COMPUTER/ELECTRONIC ACCOMMODATIONS PROGRAM (CAP): CAP USERS WHO CANNOT PHYSICALLY PERFORM CLO SHALL BE PROVIDED OTHER MEANS FOR NETWORK ACCESS. INFORMATION ON THE CAP PROGRAM CAN BE FOUND AT WWW.TRICARE.MIL/CAP.

6. AUTHORIZED CLO EXCEPTIONS FOR NON-USER ACCOUNTS: SOME SYSTEM AND OTHER UNIQUE ACCOUNTS ARE NOT ABLE TO PERFORM CLO DUE TO TECHNICAL LIMITATIONS. BELOW ARE THE TWO AUTHORIZED EXCEPTION CATEGORIES FOR NON-USER ACCOUNTS.

A. SERVICE ACCOUNTS: CLO IS NOT REQUIRED FOR SYSTEM SERVICE ACCOUNTS (COMPUTER-TO-COMPUTER ACCOUNTS; E.G., WINDOWS SERVICE ACCOUNTS AS DEFINED IN REF B) THAT PROVIDE SERVICES SUCH AS ACTIVE DIRECTORY CONNECTOR OR SQL SERVER EXPRESS.

B. SYSTEM ADMINISTRATOR ACCOUNTS FOR ADDING COMPUTERS: ALL SYSTEM ADMINISTRATORS ARE REQUIRED TO HAVE AND USE AN ALT FOR CLO; HOWEVER, A SMALL NUMBER OF SYSTEM ADMINISTRATOR ACCOUNTS WILL STILL REQUIRE THE USE OF USERNAME AND PASSWORD WHEN ADDING COMPUTERS TO A WINDOWS DOMAIN. ONLY SYSTEM ADMINISTRATOR ACCOUNTS PERFORMING THIS SPECIFIC FUNCTION ARE AUTHORIZED THE CLO EXCEPTION. THIS INCLUDES DEPLOYABLE SUPPORT PLAN UNIT IT REPRESENTATIVES. ALL OTHER SYSTEM ADMINISTRATORS MUST USE PK-ENABLED APPLICATIONS AND HAVE THEIR ACCOUNTS CLO ENFORCED.

7. ALTERNATE TOKEN, LOGICAL ACCESS TOKEN AND CLO ENABLEMENT: JTF-GNO ENCOURAGES MAXIMUM USE OF THE ALT TOKEN PER REF C WHERE CAC ISSUANCE IS NOT POSSIBLE. THE NAVY HAS DEVELOPED PROCEDURES TO ISSUE ALTS IN ORDER TO ELIMINATE CLO EXCEPTION CATEGORIES. THE CURRENT STATUS OF THE NAVY ALT PROGRAM, THE PROCESS FOR OBTAINING AN ALT, AND THE LIST OF ACCOUNT TYPES THAT MAY RECEIVE AN ALT ARE LOCATED ON THE INFOSEC WEB SITE AT

[HTTPS:\(SLASH SLASH\)INFOSEC.NMCI.NAVY.MIL/PKI/](https://(SLASH SLASH)INFOSEC.NMCI.NAVY.MIL/PKI/). THIS LIST WILL BE UPDATED AS CHANGES OCCUR. THE NAVY ALT PROGRAM WAS GREATLY EXPANDED IN NOV 2009 TO INCLUDE MANY OF THE ACCOUNT TYPES LISTED AS AUTHORIZED CLO EXCEPTIONS IN REF A. THE FOLLOWING ACCOUNT TYPES ARE NOW ELIGIBLE FOR A LOGICAL ACCESS TOKEN OR ALT TOKEN. COMMANDS WITH ALT TOKEN ELIGIBLE ACCOUNTS MUST BEGIN REQUESTING ALT TOKENS NOW, FOLLOWING GUIDANCE IN REF F. REQUESTS NOT SUBMITTED IN A TIMELY MANNER WILL NOT GET PROCESSED IN TIME TO MEET THE BELOW DEADLINES.

A. FUNCTIONAL OR ROLE-BASED ACCOUNTS: PER REF F, ADDENDUM A (ROLE-BASED CERTIFICATES), FUNCTIONAL OR ROLE-BASED ACCOUNTS MAY NOW RECEIVE AN ALT TOKEN. EXAMPLES OF FUNCTIONAL OR ROLE-BASED ACCOUNTS INCLUDE WATCHSTANDER, DUTY OR TRAINING ACCOUNTS. ALT TOKENS SHALL ONLY BE ISSUED TO FUNCTIONAL ACCOUNTS THAT ARE USED VIA NETWORK LOGON. ALT TOKENS SHALL NOT BE ISSUED TO FUNCTIONAL MAILBOXES. FUNCTIONAL MAILBOXES THAT RECEIVE EMAIL THAT MUST BE ENCRYPTED PER REF G SHALL OBTAIN EMAIL ENCRYPTION KEYS AS DOD PKI SOFTWARE CERTIFICATES. FUNCTIONAL ACCOUNTS SHALL BE CLO ENFORCED AND REMOVED FROM THE EXCEPTION LIST NO LATER THAN 06 DEC 2010.

B. SECONDARY ACCOUNTS: NON-RESERVIST USERS WITH MORE THAN ONE ACCOUNT ON THE SAME NETWORK (I.E., WINDOWS ACTIVE DIRECTORY FOREST) ARE ELIGIBLE TO RECEIVE AN ALT TOKEN FOR THEIR SECONDARY ACCOUNT. RESERVISTS SHOULD ENABLE CLO ON THEIR ACCOUNT PER THE PROCESS IN PARAGRAPH 7D. SECONDARY ACCOUNTS SHALL BE CLO ENFORCED AND REMOVED FROM THE CLO EXCEPTION LIST NO LATER THAN 11 AUG 2010.

C. FOREIGN/LOCAL NATIONALS: MOST FOREIGN/LOCAL NATIONAL PERSONNEL AUTHORIZED TO WORK ON DOD NETWORKS ARE AUTHORIZED TO RECEIVE A CAC. THOSE FOREIGN/LOCAL NATIONALS WHO ARE NOT ELIGIBLE TO RECEIVE A CAC DUE TO LOCAL RESTRICTIONS, LAWS OR REQUIREMENTS MAY NOW RECEIVE AN ALT TOKEN PER REF F, ADDENDUM E. FOREIGN LOCAL/NATIONALS CURRENTLY ON THE CLO EXCEPTION LIST SHALL BE CLO ENFORCED AND REMOVED FROM THE EXCEPTION LIST NO LATER THAN 14 JUL 2010.

D. VOLUNTEER PERSONNEL: PER REF E, VOLUNTEER PERSONNEL WITH NAVY NETWORK ACCOUNTS (E.G., OMBUDSMAN, FLAG SPOUSES) ARE ELIGIBLE FOR A LOGICAL ACCESS TOKEN. VOLUNTEER PERSONNEL WILL BE REGISTERED IN DEERS THROUGH THE CONTRACTOR VERIFICATION SYSTEM (CVS). COMMAND CVS TRUSTED AGENTS SHOULD WORK WITH THEIR SERVICING PERSONNEL SUPPORT DETACHMENT (PSD) TO SEE IF THE VOLUNTEER LOGICAL ACCESS CREDENTIAL IS AVAILABLE IN THEIR AREA. MORE INFORMATION ON CVS CAN BE FOUND AT PMO.CAC.NAVY.MIL.

E. SECONDARY RESERVIST ACCOUNTS: NAVY RESERVISTS WHO ARE ALSO CIVIL SERVANTS OR NAVY CONTRACTORS WITH MORE THAN ONE ACCOUNT ON A SINGLE NETWORK CAN ENABLE CLO ON THEIR RESERVE ACCOUNT BY ADDING THE PERSONNEL CATEGORY CODE (PCC) TO THE USER PRINCIPLE NAME (UPN) ON THEIR RESERVE CAC USING THE CAC USER MAINTENANCE PORTAL (UMP) AT [HTTP:\(SLASH SLASH\)WWW.DMDC.OSD.MIL/UMP](http://(SLASH SLASH)WWW.DMDC.OSD.MIL/UMP) (ALL LOWER CASE). FURTHER GUIDANCE ON HOW TO USE THE UMP TO ENABLE CLO WILL BE POSTED ON THE PKI PAGE OF THE INFOSEC WEB SITE. NETWORK OWNERS MUST MODIFY ANY CLO ENABLEMENT SCRIPTS AND PROCESSES TO ALLOW RESERVIST ACCOUNTS TO BE REMOVED FROM THE CLO EXCEPTION LIST VIA THE UPN MODIFICATION PROCESS NO LATER THAN 01 OCT 2010. RESERVE COMMANDS ARE ENCOURAGED TO HAVE PERSONNEL MODIFY THEIR UPN AS SOON AS POSSIBLE IN ORDER TO EXPEDITE THE CLO ENFORCEMENT PROCESS ONCE THE NETWORKS HAVE MODIFIED THEIR CLO ENABLEMENT SCRIPTS/PROCESSES.

8. OTHER EXCEPTION TYPES NOT COVERED IN THIS NTD MUST BE APPROVED BY NETWARCOM. ACCOUNTS SHALL NOT BE APPROVED AS EXCEPTIONS TO CLO BASED SOLELY UPON RANK OR POSITION. ANY CHANGES TO THE AUTHORIZED CLO EXCEPTION CATEGORIES WILL BE PUBLISHED AS AN UPDATE TO THIS NTD. ANY ENTERPRISE NETWORK SPECIFIC EXCEPTIONS WILL BE PUBLISHED VIA OTHER

MESSAGE TRAFFIC, SUCH AS NMCI INFORMATION BULLETIN (NIB) OR ONE-NET INFORMATION BULLETIN (OIB).

9. REQUIREMENT FOR CLO DOES NOT APPLY TO SIPRNET AT THIS TIME; HOWEVER, THE LONG TERM GOAL IS TO REQUIRE CLO ON BOTH NIPRNET AND SIPRNET. THIS WILL NOT BE POSSIBLE UNTIL DOD FIELDS A PKI HARDWARE TOKEN FOR THE SIPRNET, AS THE CAC IS ONLY AUTHORIZED FOR USE ON THE NIPRNET.

10. THIS NTD WILL REMAIN IN EFFECT UNTIL CANCELLED OR REPLACED. ALL EFFECTIVE NTDS MAY BE VIEWED ON THE INFOSEC WEBSITE: [HTTPS:\(SLASH SLASH\)INFOSEC.NMCI.NAVY.MIL](https://(SLASH)INFOSEC.NMCI.NAVY.MIL) UNDER THE DOCUMENTATION, NETWARCOM TABS.

11. MINIMIZE CONSIDERED. RELEASED BY MR. BRIAN BROENE, DEP NETOPS.//