

***** UNCLASSIFIED/// PRIVACY MARK UNDEFINED *****

Subject: NAVY TELECOMMUNICATIONS DIRECTIVE (NTD) 03-11, DISPOSAL OF NAVY COMPUTER

Originator: /C=US/O=U.S.

GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=VIRGINIA/L=VIRGINIA BEACH/OU=COMNAVNETWARCOM VIRGINIA BEACH VA(UC)

DTG: 021854Z May 11

Precedence: ROUTINE

DAC: General

To: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ADDRESS LISTS(UC)/CN=ALALCOM(UC)

cc: /C=US/O=U.S.

GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=VIRGINIA/L=VIRGINIA BEACH/OU=COMNAVNETWARCOM VIRGINIA BEACH VA(UC)

UNCLASSIFIED//

ALCOM 083/11

MSGID/GENADMIN/NETWARCOM/CIO/MAY//

SUBJ/NAVY TELECOMMUNICATIONS DIRECTIVE (NTD) 03-11, DISPOSAL OF NAVY COMPUTER HARD DRIVES//

REF/A/GENADMIN/COMNAVNETWARCOM/241600ZNOV2008//

REF/B/GENADMIN/DON CIO WASHINGTON DC/221633Z AUG2010//

REF/C/DOC/OPNAV/31MAY2000//

REF/D/DOC/NAVAUDIT/29APR2009//

REF/E/ DOC/SECNAV/30JUN2006//

REF/F/DOC/DRMS/12MAY2008//

NARR/REF A IS NTD 12-08, DISPOSITION OF NAVY COMPUTER HARD DRIVES. REF B IS DEPARTMENT OF THE NAVY (DON) CHIEF INFORMATION OFFICER (CIO) MESSAGE PROCESSING OF MAGNETIC HARD DRIVE STORAGE MEDIA FOR DISPOSAL. REF C IS OPNAV INFORMATION ASSURANCE REMANENCE SECURITY PUBLICATION. REF D IS NAVAL AUDIT SERVICE REPORT N2009-0027. REF E IS SECRETARY OF THE NAVY (SECNAV) INSTRUCTION M-5510.36, DON INFORMATION SECURITY PROGRAM. REF F IS DEFENSE REUTILIZATION MATERIAL SYSTEM 4160.14 OPERATING INSTRUCTIONS FOR DISPOSITION MANAGEMENT//

POC/JULIANA ROSATI/CDR/OPNAV N2N6F15B/TEL: 571-256-8523

/EMAIL:JULIANA.ROSATI(AT)NAVY.MIL//

POC/FREDDIE BLASER/CIV/NETWARCOM/TEL:757-417-6798(X2)

/EMAIL:FREDDIE.BLASER(AT)NAVY.MIL//

RMKS/1. PURPOSE. CANCEL REF A. THIS NTD ESTABLISHES NAVY IMPLEMENTATION POLICY FOR REF B.

2. APPLICABILITY AND SCOPE. THIS POLICY APPLIES TO ALL NAVY COMMANDS USING COLLATERAL CLASSIFIED (E.G. SIPRNET, SDREN) AND UNCLASSIFIED (E.G., NMCI, ONE-NET, IT21, DREN, EXCEPTED, AND LEGACY) NAVY NETWORKS INTERNAL AND REMOVABLE MAGNETIC DRIVES, AND STAND ALONE DEVICES. THIS INCLUDES, BUT IS NOT LIMITED TO, STORAGE AREA NETWORK (SAN) DEVICES, SERVERS, WORKSTATIONS, LAPTOPS/NOTEBOOKS, PRINTERS, COPIERS, SCANNERS, AND MULTI-FUNCTION DEVICES (MFD) WITH INTERNAL HARD DRIVES, REMOVABLE HARD DRIVES, AND EXTERNAL HARD DRIVES. FROM THIS POINT FORWARD THIS NTD WILL REFER TO THESE DEVICES COLLECTIVELY AS HARD DRIVES. THE NEXT REVISION OF REF C WILL UPDATE THE PROCEDURES OUTLINED IN THIS NTD. A FUTURE NMCI INFORMATION BULLETIN (NIB) WILL PUBLISH NMCI-UNIQUE PROCEDURES. NOTHING IN THIS NTD SHALL ALTER OR SUPERSEDE DON AUTHORITIES AND POLICIES.

3. BACKGROUND. REF D IDENTIFIED DEFICIENCIES IN SAFEGUARDING AND DESTRUCTION REQUIREMENTS FOR NAVY HARD DRIVES. FAILURE TO FOLLOW PROPER DON POLICY FOR SAFEGUARDING AND MEDIA PHYSICAL DESTRUCTION TECHNIQUES (OUTLINED IN REF B) INCREASES POTENTIAL FOR A COMPROMISE OF NATIONAL SECURITY INFORMATION OR

BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII). PROCEDURES OUTLINED IN THIS MESSAGE ARE DESIGNED TO MITIGATE THAT RISK THROUGHOUT THE NAVY.

4. ACTION. ALL HARD DRIVES THAT HAVE BEEN USED IN NAVY CLASSIFIED OR UNCLASSIFIED NETWORKS ARE THE PROPERTY OF THE NAVY, SPECIFICALLY THE COMMAND TO WHICH USERS OF THAT HARD DRIVE ARE ASSIGNED, AND SHALL BE THE RESPONSIBILITY OF THAT COMMAND.

A. COMMANDS SHALL ENSURE THAT ALL COLLATERAL CLASSIFIED HARD DRIVES ARE DEGAUSSED AND PHYSICALLY DESTROYED IAW PARAGRAPH 5.

B. COMMANDS SHALL ENSURE THAT UNCLASSIFIED HARD DRIVES USED IN NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS) OR NAVY NUCLEAR PROPULSION INFORMATION (NNPI) COMMUNITY OF INTEREST (COI) ARE DEGAUSSED AND PHYSICALLY DESTROYED IAW PARAGRAPH 5.

C. COMMANDS SHALL ENSURE DESTRUCTION OF UNCLASSIFIED HARD DRIVES IAW PARAGRAPH 5. DEGAUSSING IS NOT REQUIRED. IAW PARAGRAPH 7, COMMANDS MAY REQUEST A DON DEPUTY CIO NAVY (DDCIO(N)) WAIVER FROM THIS DESTRUCTION REQUIREMENT IN CASES THAT AN APPROVED DAR SOLUTION WITH FULL DISK ENCRYPTION HAS BEEN IMPLEMENTED.

5. APPROVED METHODS OF DESTRUCTION. THE PREFERRED METHOD FOR DESTRUCTION IS TO SHIP THE HARD DRIVE(S) TO THE NATIONAL SECURITY AGENCY (NSA) FOR DEGAUSSING AND CRUSHING. NSA ACCEPTS BOTH UNCLASSIFIED AND CLASSIFIED HARD DRIVES FOR DESTRUCTION SUBJECT TO PROCESSING CAPACITY. COMMANDS MUST STRICTLY ADHERE TO NSA-DIRECTED TURN- IN INSTRUCTIONS. THESE INSTRUCTIONS ARE AVAILABLE FOR DOWNLOADED FROM: WWW.NSA.GOV/CMC. SHIPMENT METHODS IDENTIFIED IN THE NSA CLASSIFIED MATERIAL CONVERSION WEB PAGE ARE IN COMPLIANCE WITH DON GUIDELINES FOR CONUS AND OCONUS SHIPMENT (REF D REFERS). COMMANDS ARE RESPONSIBLE FOR ALL SHIPPING COSTS AND COMMANDS SHALL RETAIN DOCUMENTATION OF DESTRUCTION IAW PARA 6.

A. COMMANDS MAY CHOOSE FROM SEVERAL ALTERNATIVES TO THE SHIPMENT METHOD DESCRIBED ABOVE. FIRST, COMMANDS ARE AUTHORIZED TO DEGAUSS CLASSIFIED HARD DRIVES LOCALLY USING AN NSA APPROVED DEGAUSSER. THE NSA EVALUATED PRODUCTS LIST OF APPROVED DEGAUSSERS IS AVAILABLE FOR DOWNLOADED FROM WWW.NSA.GOV/IA/_FILES/GOVERNMENT/MDG/EPL-DEGAUSSER25FEBRUARY2010.PDF. COMMANDS MUST ALSO ENSURE PHYSICAL DESTRUCTION OF CLASSIFIED AND UNCLASSIFIED HARD DRIVES, IN A MANNER THAT PROVIDES 100 PERCENT ASSURANCE THE DEVICE AND/OR INFORMATION IS NOT RECOVERABLE. IAW PARA 4 OF REF B, DESTRUCTION METHODS INCLUDE SHREDDING, CRUSHING, BURNING, OR MELTING. DETAILS ARE AVAILABLE AT WWW.DON.CIO.NAVY.MIL/PRIVACY. COMMANDS SHALL RETAIN DOCUMENTATION OF DESTRUCTION IAW PARA 6.

B. AS A SECOND ALTERNATIVE, COMMANDS MAY SHIP HARD DRIVES TO ANOTHER NAVY COMMAND OR CLEARED CONTRACTOR FACILITY WITH DEGAUSSING AND PHYSICAL DESTRUCTION (AS APPLICABLE) CAPABILITY DESCRIBED IN PARA 5A. DETAILS ON CONTRACTOR FACILITIES ARE AVAILABLE AT WWW.DONCIO.NAVY.MIL/PRIVACY. COMMANDS ARE RESPONSIBLE FOR ALL SHIPPING AND CONTRACTOR PROCESSING COSTS. COMMANDS SHALL RETAIN DOCUMENTATION OF DESTRUCTION IAW PARA 6.

C. A THIRD ALTERNATIVE IS DESTRUCTION THROUGH THE DEFENSE LOGISTICS AGENCY (DLA) DISPOSITION SERVICE. DETAILS ON THE DLA PROCESS ARE OUTLINED IN REF F, AVAILABLE AT WWW.DRMS.DLA.MIL. COMMANDS SHALL RETAIN DOCUMENTATION OF DESTRUCTION IAW PARA 6.

6. ACCOUNTABILITY, CONTROL AND DESTRUCTION. ALL COMMAND HARD DRIVE DISPOSITION RECORDS, TO INCLUDE THOSE WITH A WAIVER FROM DESTRUCTION, MUST BE RETAINED BY THE COMMAND FOR 2 YEARS AS PART OF REF B AUDITING RECORDS REQUIREMENTS. SAMPLE LOG TEMPLATES FOR BOTH HD DESTRUCTION AND HD RETURN UNDER A WAIVER MAY BE FOUND AT [HTTPS:\(SLASH SLASH\) WWW.PORTAL.NAVY.MIL/NETWARCOM/CIO/DEFAULT.ASPX](https://WWW.PORTAL.NAVY.MIL/NETWARCOM/CIO/DEFAULT.ASPX) UNDER WHATS HOT LINKS.

A. UPON REMOVAL OF A HARD DRIVE FROM A NETWORK OR A STANDALONE PIECE OF EQUIPMENT, A REPRESENTATIVE DESIGNATED BY THE COMMANDING OFFICER (E.G. COMMAND SECURITY MANAGER, COMMAND IAM ETC.), SHALL MAINTAIN ACCURATE RECORDS

DOCUMENTING THE DEGAUSSING/PHYSICAL DESTRUCTION OF EACH HARD DRIVE. DOCUMENTATION SHALL INCLUDE MANUFACTURER SERIAL NUMBER, ASSET TAG NUMBER, TYPE, MODEL, AND CLASSIFICATION. LOCAL ACCOUNTABILITY RECORDS USING A DATABASE OR LOGBOOK ARE MANDATORY AND MUST ASSOCIATE THE HARD DRIVE TO A SPECIFIC COMPUTER/DEVICE AND USER, AS APPLICABLE. COMMANDS SHALL ENSURE HARD DRIVES ARE PROPERLY SECURED (IAW REF D FOR CLASSIFIED DRIVES) AND MAINTAIN A CHAIN OF CUSTODY UNTIL PHYSICALLY DESTROYED, SHIPPED TO AN APPROVED DESTRUCTION FACILITY, OR OTHERWISE DISPOSED OF PER THE SPECIFICATIONS OF A WAIVER.

B. IN THE CASE OF NMCI AND OTHER SERVICE CONTRACTS, ALL CLASSIFIED AND UNCLASSIFIED HARD DRIVES THAT HAVE BEEN PUT INTO SERVICE ARE PROPERTY OF THE US GOVERNMENT AND SHALL NOT BE TURNED OVER TO ANY CONTRACTOR DURING TECH REFRESH OR REPLACEMENT. ALL DISPOSITION AND LOGGING/ACCOUNTING RESPONSIBILITIES FOR SUCH HARD DRIVES REMAIN WITHIN THE GOVERNMENT AND SHALL BE CARRIED OUT IAW THIS DIRECTIVE AND ANY ADDITIONAL COI SPECIFIC REQUIREMENTS. UNCLASSIFIED HARD DRIVES WITH APPROVED WAIVERS (PARA 7) MAY BE TURNED OVER TO NMCI PRIMARY CONTRACTOR OR OTHER SERVICE CONTRACT VENDORS. REGARDLESS, BOTH SERVICE CONTRACT PRIMARY VENDOR AND THE OWNING COMMAND SHALL MAINTAIN LOCAL CUSTODY LOGS OF ALL HARD DRIVES FOR TWO YEARS, WHETHER RETAINED BY THE VENDOR FOR RECYCLING UNDER A WAIVER OR RETAINED BY CUSTOMER COMMAND FOR DESTRUCTION.

7. WAIVERS FROM HARD DRIVE DESTRUCTION REQUIREMENT. CLASSIFIED HARD DRIVES AND UNCLASSIFIED NCIS AND NNPI COI HARD DRIVES ARE NOT ELIGIBLE FOR A WAIVER FROM THE PHYSICAL DESTRUCTION REQUIREMENT. WAIVERS OF HARD DRIVE DESTRUCTION FOR UNCLASSIFIED, NON-NNPI, NON-NCIS EQUIPMENT MAY BE REQUESTED FROM (DDCIO(N)), THE NAVY WAIVER APPROVAL AUTHORITY. WAIVER REQUESTS SHALL FULLY ADDRESS REQUIREMENTS IDENTIFIED BELOW AND SHALL INCLUDE COST ANALYSIS OF ALTERNATIVES. SUBMIT WAIVER REQUESTS TO THE OPNAV POC LISTED IN THIS MESSAGE. WAIVER REQUESTS SHALL INCLUDE A DESCRIPTION OF HOW THE FOLLOWING CONDITIONS WILL BE MET:

A. THE HOST NETWORK MUST HAVE IMPLEMENTED A DON APPROVED DATA AT REST (DAR) SOLUTION WITH FULL DISK ENCRYPTION ACROSS THE NETWORK. A SINGLE WAIVER MAY APPLY TO A HOST NETWORK WITH A DAR SOLUTION DEPLOYED.

B. COMPUTER HARD DRIVES ENCRYPTED WITH A DON APPROVED DAR SOLUTION MUST BE INDIVIDUALLY TESTED WHILE STILL IN DON POSSESSION AND PRIOR TO RELEASE FROM GOVERNMENT CONTROL TO VERIFY NO DATA IS READABLE. DESIGNATED COMMAND REPRESENTATIVES MUST RETAIN DOCUMENTATION/LOGS THAT DRIVES WERE INDIVIDUALLY TESTED.

C. FOR STAND ALONE OR NETWORK COPIERS, PRINTERS, AND MFDS, THE HARD DRIVES MUST BE ENCRYPTED USING FIPS 140-2 CERTIFIED SOFTWARE.

D. REQUESTING COMMAND SHALL GIVE JUSTIFICATION OF WHY PHYSICAL DESTRUCTION IS NOT FEASIBLE OR IN THE BEST INTEREST OF THE GOVERNMENT AND INCLUDE A DESCRIPTION OF ALTERNATIVE MITIGATING MEASURES (E.G. OVERWRITE OF HD) TO PREVENT DATA RECOVERY AND EXPLOITATION FOLLOWING REMOVAL FROM NAVY CONTROL.

E. WAIVER REQUESTS SHALL BE ENDORSED BY AN ECH II FLAG OFFICER OR SES PRIOR TO SUBMISSION TO DDCIO(N).

8. OVERSIGHT. ALL COMMANDS ARE SUBJECT TO INSPECTIONS BY APPROPRIATE AUTHORITIES TO ENSURE COMPLIANCE (E.G., NAVAL AUDIT SERVICE, DISA COMMAND CYBER READINESS INSPECTION (CCRI) ETC.). ECHELON II COMMANDERS ARE RESPONSIBLE FOR ENSURING THAT INTERNAL MANAGEMENT CONTROLS ARE IN PLACE TO MONITOR AND MAINTAIN COMPLIANCE WITH THIS POLICY.

9. THIS NTD WILL REMAIN IN EFFECT UNTIL CANCELED OR REPLACED. THE AUTHORITATIVE SITE FOR ALL EFFECTIVE NTDS IS THE NETWARCOM CIO PORTAL. NTDS ARE ALSO POSTED ON THE INFOSEC WEBSITE. BOTH SITES ARE PKI/CAC ENABLED.

A. HTTPS:(SLASH

SLASH)WWW.PORTAL.NAVY.MIL/NETWARCOM/CIO/POLICYDIRECTION/DEFAULT.ASPX

B. HTTPS:(SLASH SLASH) INFOSEC.NMCI.NAVY.MIL

C. HTTPS:(SLASH SLASH) INFOSEC.NAVY.MIL

NOTE: FROM THE INFOSEC SITE, CLICK ON THE DOCUMENTATION TAB, AND SELECT NETWARCOM.

10. REQUEST WIDEST DISSEMINATION PARTICULARLY TO COMMAND SECURITY MANAGER, COMMAND IA MANAGER AND NMCI CONTRACTOR REPRESENTATIVE (CTR) OR EQUIVALENT.//

Classified by:

Reason:

Declassify On: