DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5230.8B
N6
7 Jan 2019

CNATRAINST 5230.8B

From: Chief of Naval Air Training

Subj: MISSION DATA TRANSFER UNIT CONTROL PLAN

Ref: (a) USCYBERCOM CTO 10-084
(b) SECNAVINST 5239.19 Department of the Navy Computer Network Incident Response and Reporting Requirements
(c) DoDI 8500.01 Cybersecurity
(d) DoDI 8500.2 Information Assurance Implementation
(e) NIST Special Publication 800-88, Revision 1, Guideline for Media Sanitization
(f) DON CIO MSG 281759Z AUG 2012
(g) SECNAVINST 7320.10A DON Personal Property Policies and Procedures
(h) SECNAVINST 5239.3B Department of the Navy Information Navy Information
(i) DoDI 8510.01 Risk Management Framework for DOD Information Technology

Encl: (1) List of Acronyms and Abbreviations
(2) MDTU USB Controlling Custodian/End User Agreement
(3) MDTU USB Device Inventory Control Sheet
(4) MDTU/MDS/DFPS/JMPS Weekly AV Scan Log
(5) List of Web Links to References

1. Purpose

a. To provide Cybersecurity policy and proper operation guidelines for Mission Data Transfer Unit (MDTU) implementation and operation at the Chief of Naval Air Training (CNATRA) squadrons to meet the requirements of references (a) through (i).

b. To meet the requirements of National Institute of Standards and Technology (NIST) and exercise positive control of the MDTU used in CNATRA for audio/video/data download from the Digital Data Set (DDS) Control Panel (CP) and used for post mission aircrew debrief, enhanced maintenance troubleshooting, and the periodic upload of navigational waypoints.

2. Cancellation. CNATRAINST 5230.8A

3. Acronyms. Enclosure (1) of this instruction defines relevant terms.

4. Objectives

a. To establish user responsibilities for the proper use of MDTUs.

b. To establish processes for physical custody of MDTUs.

c. To establish process for replacement and disposal of MDTUs.

5. Scope. MDTUs are an integral asset for post mission aircrew debrief of Student Naval Aviators and Student Naval Flight Officers under training at home bases and deployed sites, both ashore and afloat. All MDTUs shall be controlled and maintained as defined in CTO 10-084 and this instruction. CTO 10-084 references multiple documents and requirements that also require compliance.

6. Background

a. On 14 November 2008, Commander, United States Strategic Command (CDRUSSTRATCOM) suspended the use of memory sticks, thumb drives and camera memory cards (hereafter referred to collectively as flash media), most commonly connected via Universal Serial Bus (USB) ports on all Department of Defense(DoD) Non-Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS) computers using Windows Operating Systems (OS) due to a severe security risk to the Global Information Grid (GIG).

b. Prior to the suspension, PMA-273 was exercising a small business initiative to develop a next generation flight data recorder for the T-45 community and potentially as a common avionics solution for other platforms to meet Navy and DOD requirements for crash survivable memory and mitigate obsolescence issues with the current recorders. The DDS previously utilized a United States Naval Network Warfare Command (USNETWARCOM) waivered USB flash memory device, for removal of audio/video for mission debrief and the upload of navigation waypoints. This function will be performed by a hardened, encrypted, FIPS-140 data-at-rest compliant USB device herein after referred to as the MDTU. Additionally, the MDTU could be utilized to download flight data sets for analysis and enhancement of post flight maintenance troubleshooting if the normal method of download is precluded.

c. Post mission aircrew debriefs are conducted utilizing a stand-alone laptop computer, referred to herein after as the Mission Debrief Station (MDS), located in aircrew brief/debrief spaces. Navigational waypoints are generated using the Almanac Loading Software (ALS) loaded on Digital Flight Planning System (DFPS) or Joint Mission Planning System (JMPS) computers, which are both stand-alone work stations for flight planning. The MDTU shall only be utilized with the MDS, DFPS, JMPS and aircraft.

d. The DDS utilizes a real-time operating system manufactured by Green Hills Software. However, navigation waypoints are generated by DFPS which was developed by Joint Systems Support Activity (JSSA) at Naval Air Warfare Center – Weapons Division (NAWCWD) China Lake, California. The DFPS is a stand-alone work station that operates in a Microsoft Windows environment, and writes the navigational waypoints to the MDTU for upload to the DDS. The MDS is a stand-alone laptop running Windows OS for playback of recorded flight video. The JMPS laptops are stand-alone laptops running Windows Operating System (OS), provided by PMA-281 for flight planning purposes.

e. Reference(a)defines specific requirements for the use of USB devices within DOD on computers using the Windows operating system due to a severe security risk.

7. Fundamental MDTU Policy. MDTU use is limited to:

a. Download of audio/video from the DDS-equipped T-45 aircraft for mission debrief; playback should be accomplished on the MDS.

b. Upload of navigational waypoints utilizing the government provided DFPS or JMPS computers.

c. Download of such flight data files as to facilitate maintenance.

d. Official use only.

e. UNCLASSIFIED data only.

8. User Responsibilities. All users shall sign a user agreement, enclosure (2), and a System Authorization Access Request - Navy (SAAR-N)(OPNAV 5239/14). All users shall report any incidents of misuse, loss or theft of an MDTU. Reports shall be made to the Information Systems Security Officer (ISSO) and the chain of command.

9. Password Protection. The MDTUs require a unique password to be:

a. Case sensitive

b. Minimum of 14 characters

c. Characters mix should include at least one upper case letter, lower case letter, number, and special character.

d. Updated quarterly

e. Reset by the ISSO as required

10. Physical Custody by a Controlling Custodian. Controlling custodians shall perform custodial duties when acting as a Squadron, Wing or Detachment Duty Officer or Assistant Duty Officer. MDTUs shall be maintained by a controlling custodian and/or end user to prevent compromise of the device. When not in use, MDTUs shall be maintained in secure facilities. When issuing an MDTU to aircrew, an inventory control sheet, enclosure (3), shall be used by the controlling custodian in order to maintain inventory and strict control of checked out MDTUs throughout the useful life of the MDTU. The inventory control sheet should also be used to document custody transfer of MDTUs during change of controlling custodian/WDO during watch transfer. The control sheet shall have at a minimum:

a. Serial Number

b. Crew Name, printed

c. Date/Time Out

d. Crew Signature Out

e. Duty Officer/Custodian Name

f. Expected Duration/Comments

g. Date/Time Return

h. Crew Signature Return

i. Duty Officer/Custodian Name

11. Scanning Software. The anti-virus (AV) software resides on DFPS, MDS, and JMPS computers. The MDTU will be scanned by the computer with each use. The ISSO will verify the AV definitions are updated weekly on client workstations, enclosure (4). Devices found to be infected shall be reported and surrendered to the ISSO.

a. The ISSO shall initiate an investigation and report the results to the Information Security Systems Manager (ISSM) and the chain of command.

b. MDTUs are not to be reformatted until directed to do so by the ISSM.

c. Infected MDTUs require that the ISSO create an incident ticket with the Joint Cert Database with the subject field titled 'Infected MDTU', references (a) and (b).

12. Labeling and Tracking MDTUs. The ISSO shall ensure each MDTU has been clearly labeled and traceable by its serial number. Each MDTU:

a. Must include a serial number that is easily readable.

b. Shall be clearly labeled with an appropriate classification marking (Unclassified).

c. Shall be stored, transported, and destroyed in accordance with reference (c).

d. Shall Be distributed and tracked by the controlling custodian. The controlling custodian will use enclosure (3) for the tracking and distribution to the user.

13. Disposal and Destruction. Disposal and destruction will be in accordance with references (c) through (f).

14. Lost MDTUs. Lost MDTUs shall be reported to the ISSO. Lost MDTUs will be handled in accordance with references (b) and (g).

15. Action. COs for CNATRA commands that utilize the MDTUs shall implement and adhere to this policy.

16. Reports

a. Controlling custodians shall submit all MDTU USB Controlling Custodian/End User Agreements and MDTU USB Device Inventory Control Sheets to the ISSO at the completion of each work week during home field operations and upon return to home field following detachment operations.

b. ISSOs will submit a MDTU monthly report to the ISSM to include:

(1) MDTU USB End User Agreements, enclosure (2).

(2) MDTU USB Device Inventory Control Sheets, enclosure (3).

(3) MDTU/MDS/DFPS/JMPS Weekly AV Scan Logs, enclosure (4).

17. Review and Effective Date. *(Required)* Per OPNAVINST 5215.17A, (organization title) will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after the effective date unless reissued or cancelled prior to the 5-year anniversary date, or an extension has been granted.

18. Contact Information for CNATRA CIO: CNATRA (N6), 9035 Ocean Drive, Suite 322, Corpus Christi, TX 78419, DSN 861-3213 or Commercial (361) 961-3213.

19. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 series.

20. Review and Effective Date. Per OPNAVINST 5215.17 series, CNATRA will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

S. B. STARKEY
Chief of Staff

Distribution:
CNATRA SharePoint and CNATRA Website

LIST OF ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AV	Anti-virus
CDRUSSTRATCOM	Commander, United States Strategic Command
CIO	Chief Information Officer or Command Information Officer
CNATRA	Chief of Naval Air Training
CO	Commanding Officer
CP	Control Panel
CTO	Computer Task Order
DDS	Digital Data Set
DFPS	Digital Flight Planning System
DOD	Department of Defense
DODI	Department of Defense Instruction
DON	Department of the Navy
FIPS	Federal Information Processing Standard
GIG	Global Information Grid
IA	Information Assurance
ISSM	Information Systems Security Manager (at CNATRA N6)
ISSO	Information Systems Security Officer (at TW)
IT	Information Technology
JMPS	Joint Mission Planning System
JSSA	Joint Systems Support Activity
JWICS	Joint Worldwide Intelligence Communication Systems
MDS	Mission Debrief Station
MDTU	Mission Data Transfer Unit
NAWC-WD	Naval Air Warfare Center – Weapons Division
NIPRNET	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet

Acronym	Definition
OS	Operating System
PMA-273	Program Office, specific
PMA-281	Program Office, specific
RMF	Risk Management Framework
SAAR-N	System Authorization Access Request - Navy
SECNAVINST	Secretary of the Navy Instruction
SIPRNET	Secure Internet Protocol Network
T-45	Aircraft type
USB	Universal Serial Bus
USCYBERCOM	United States Cyber Command
USNETWARCOM	United States Naval Network Warfare Command

MDTU USB CONTROLLING CUSTODIAN/END USER AGREEMENT

1. This agreement is required to meet the requirements of USCYBERCOM Computer Tasking Order (CTO) 10-084 and to exercise positive control of the USB devices (hereafter referred to as MDTU's) used in the Chief of Naval Air Training (CNATRA) subordinate commands for audio/video/data download from the Digital Data Set (DDS) Control Panel (CP) and used for post mission aircrew debrief, enhanced maintenance troubleshooting, and the periodic upload of navigational waypoints.

2. Vigilance is required by all personnel to prevent unintentional or malicious introduction of any virus or malware into Department of Defense (DOD) computer systems. While the use of MDTU's is necessary for T-45 operations, strict adherence to the CNATRA control plan and CTO 10-084 is required to ensure security.

3. Any audio/video/data downloaded from any aircraft involved in a reportable incident/mishap is the property of the United States Government, the Aviation Mishap Board or the Naval Safety Center and may not be used or released to anyone except the senior board member, the Naval Safety Center representative, or their investigative agents.

4. By signing this end user agreement, the undersigned agrees to use the provided MDTU only in the capacity for which it is provided. That capacity is limited to download/upload of audio/video/data between the MDTU and Digital Flight Planning System (DFPS), Mission Debrief Station (MDS), Joint Mission Planning System (JMPS), or the aircraft. At no time may the MDTU be inserted into any government network computer (NMCI or other). Additionally, the MDTU shall be retained in positive control by the signee, and reported immediately if lost or stolen. The user also agrees not to use MDTU's for unauthorized purposes. The uploading of any downloaded audio/video/data to any social media website is strictly prohibited.

5. By signing this agreement, the undersigned affirms they have read and familiarized themselves with CNATRAINST 5230.8A, specifically MDTU end user and controlling custodian responsibilities, and are hereby designated a controlling custodian while standing assigned duty for the command. This designation is rescinded upon detachment from your current squadron.

_____ _____

CONTROLLING CUSTODIAN/End User Name & Signature Date

MDTU USB DEVICE INVENTORY CONTROL SHEET

Serial Number	Crew Name Print	Date/ Time Out	Crew Signature Out	Duty/ Custodial Name	Expected Duration /Comments	Date/ Time Return	Crew Signature Return	Duty/ Custodial Name

Enclosure (3)

MDTU/MDS/DFPS/JMPS WEEKLY AV LOG

Date	MDTU/MDS/DFPS/JMPS	Serial Number	Performed By	Remarks

LIST OF WEB LINKS TO REFERENCES

USCYBERCOM CTO 10-084
https://www.stigviewer.com/stig/removable_storage_and_external_connections/2015-01-26/finding/V-22110

SECNAVINST 5239.19 Department of the Navy Computer Network Incident Response and Reporting Requirements
https://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.19.pdf

DoDI 8500.01 Cybersecurity
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DoDI 8500.2 Information Assurance Implementation
http://www.prim.osd.mil/Documents/DoDI_8500-2_IA_Implementation.pdf

NIST Special Publication 800-88, Revision 1, Guideline for Media Sanitization
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

DON CIO MSG 281759Z AUG 2012
www.doncio.navy.mil/Download.aspx?AttachID=3395

SECNAVINST 7320.10A DON Personal Property Policies and Procedures
https://doni.daps.dla.mil/Directives/07000%20Financial%20Management%20Services/07-300%20General%20Accounting%20Services/7320.10A.pdf

SECNAVINST 5239.3B Department of the Navy Information Assurance Policy
https://fas.org/irp/doddir/navy/secnavinst/5239_3b.pdf

DoDI 8510.01 Risk Management Framework for DoD Information Technology
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf