



UNITED STATES MARINE CORPS

I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

IN REPLY REFER TO:
5239
SEC/IAM/jmg
27 Jan 11

POLICY LETTER 1-11

From: Chief of Staff, I Marine Expeditionary Force
To: Distribution List

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

Ref: (a) CTO 10-133 USCYBERCOM FORT MEADE, 27 NOV 10
(b) MARADMIN 683/10
(c) SECNAV M-5510.36
(d) DoD Directive 8500.1 Information Assurance (IA),
24 Oct 02
(e) DoD Instruction 8500.2 Information Assurance (IA)
Implementation, 6 Feb 03
(f) EIAD-008 V1.1 Secure Data Transfer, 2 Jun 04
(g) I MEF Policy 06-10 Hard Disk Drive, 3 Dec 09
(h) I MEF Order P5510.1D Information and Personnel
Security Program, 18 Nov 09

Encl: (1) Removable Media Classified Record of Transfer (RMCRT)
(2) SIPRNET Write to Removable Media Exemption Request
(3) Classified Material Transfer of Custody

1. Purpose. Establish the procedures for the transfer of electronic data from classified information systems to removable storage media in accordance with references (a) and (b). This policy is developed to outline the procedures and forms the I Marine Expeditionary Force Command Element (I MEF CE) and its subordinate commands will be required to execute at a minimum.

2. Background. Because of the significant risk that removable media presents to Classified Military Information USCYBERCOM has established procedures for the proper handling and transferring of classified data using all forms of removable media on SIPRNET.

3. Scope. This policy applies to all military, civilian, and contracted support personnel assigned to the I Marine Expeditionary Force and its Major Subordinate Commands (MSC).

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

4. Definition. Removable media is defined in reference (a) as CD, DVD, secure digital (SDO cards, tape, flash memory data storage devices, multimedia cards (MMC), removable hard disk drives (HDD)). For this policy removable HDD's are those devices commonly referred to as external HDD's that connect to systems normally via a USB cable and not those inbedded in the computer.

5. Policy. Each command or department will maintain human oversight in the form of an O-6 level (or by billet/command) approval authority to allow classified write access on removable media. These individuals are responsible for ensuring the requirement to move the data is justified, and to authorize, in writing specific individuals and classified systems to perform the action. Additionally the commands shall ensure that all transfers are documented and tracked in accordance with this policy. The procedures detailed within this policy will be adhered to for all classified data transfers in garrison or tactical environments.

6. Execution

a. The requirement to move media from one classified device to another is identified as a requirement by the authorized officer. The AC/S and DAC/S of of Principal and Special Staff sections, Commanding and Executive Officers of Regiments, Groups, Battalions, and Squadrons within I MEF are authorized to designate two individuals and two computers in writing to perform the classified removable media write capability in support of the mission and command functions. Those individuals and systems must be appointed in writing utilizing enclosure (2).

b. The Marine Forces Pacific AC/S G-6 or I MEF AC/S G-6 will act as the local approving Designated Approving Authority (DAA) for classified computers requesting exemption and enabling write capability on enclosure (2).

c. A copy of enclosure (2) shall be provided to the Command Security Manager once it has been fully completed for file retention in accordance with reference (b). The form must be kept on file for 5 years.

d. Personnel designated to execute transfers must complete training at website <https://dodiisclear.dia.mil/mainpage.htm> as listed on page two of enclosure (2). A copy of the certificate

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

7. Process. The designated process supporting the requirement to write classified removable media is outlined below.

a. The section or individual requesting the transfer of information to removable media will fill out boxes 1, 2, 3 and 4 of enclosure (1) and submit for review to the appropriate approval authority.

b. The AC/S and DAC/S of of Principal and Special Staff sections, Commanding and Executive Officers of Regiments, Groups, Battalions, and Squadrons shall have the authority to approve the transfer of information from classified systems to removable storage devices using enclosure (1).

c. The individual authorized to transfer information to removable media shall ensure enclosure (1) is completely filled out by the requestor and the authorized approval authority prior to execution and any document not listed on enclosure (1) shall not be transferred.

d. A copy of enclosure (1) shall be kept by each command while the removable media exists and for an additional two years after the device has been destroyed. Sections within I MEF shall keep a file copy of enclosure (1) and provide a copy to the Command Security Manager within 72 hours of creation to ensure proper control and accountability.

e. Once the media is transferred and documented on enclosure (1) the individual who transferred the media will send an email to the I MEF or MSC Information Assurance Manager (IAM) documenting the transfer.

f. If movement to a non-US secret level system is authorized, use data transfer procedures provided in the "CLEAR" training/tool. Link to the "CLEAR" training application is <https://dodiisclear.dia.mil/mainpage.htm>.

8. Marking

a. External classified HDD's shall be marked in accordance with reference (g) and the units internal marking procedures.

b. Commands will use cd/dvd labels to list the Unit Title, section requesting the CD or DVD, control number of the CD or DVD, date of creation (YYYYMMDD), and identify the device as a CD, DVD, or other. Each command shall determine which section(s) or office(s) will apply the labels. Those with the

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

authority to burn CD's and DVD's within the I MEF CE shall be responsible to apply the labels immediately following the creation of a new CD or DVD. The I MEF Command Security Manager shall provide the appropriate template and format.

c. CD's and DVD's shall be marked with a control number scheme approved by each commands Security Manager or CMCC custodian respectively.

(1) Control numbers within the I MEF CE will consist of the sections abbreviated office code, four digit year and three digit numeric number (examples: PAO+2011+001=PAO2011001 or G8+2011+001=G82011001).

(2) Those with the authority to burn CD's and DVD's within the I MEF CE shall be responsible to generate the control number in accordance with this policy.

d. The control number must be listed on enclosure (1).

9. Physical Security. Each computer that has the ability to write to removable media must be tracked and controlled by the responsible command and/or section. It is recommended that these computers be kept in safes or vaults that have limited access. The computers designated must not be made available for common use.

10. Tracking

a. Commands shall be required to account for all removable media on a monthly basis in writing.

b. Security Manager's or CMCC's, as appropriate, shall generate a database of controlled CD's and DVD's, based on enclosure (1) submissions, in order to manage the monthly audit requirement.

c. The Security Manager or CMCC shall be responsible to initiate, collect and retain a record of all monthly audits for two years. Within I MEF each Section Security Representative (SSR) shall be responsible to execute a monthly audit report produced by the Command Security Manager.

d. Enclosure (3) shall be used whenever a removable storage device is transferred to another unit. At a minimum the audit reports will list the section that manages the cd or dvd, control number, classification, date created, medium type,

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

building and storage location (vault or safe serial number or secure room number).

11. Destruction

a. Enclosure (1) must be filled out and retained for 2 years. The destruction portion of enclosure (1) shall be filled out by the individual executing the destruction or who is accepting the medium for destruction on behalf of the command.

b. Commands must identify destruction procedures for all controlled removable media. Within the I MEF Command Element only the Command Security Manager will be authorized to destroy controlled CD's, DVD's and HDD's with the exception of the I MEF G2 Special Security Officer (SSO) retaining the authority to destroy only G2 controlled CD's and DVD's.

12. Existing Media. Within 30 days of this policy letter's approval existing removable media (CD's, DVD's and HDD's) containing classified information shall be accounted for and controlled if the information/data is required or destroyed in accordance with this policy within 30 days of this policy letter's approval. Controlling of existing media will include filling out a copy of enclosure (1) for each removable storage device.

13. Alternate Methods of transfer. I MEF and the Major Subordinate Commands maintain an email capability and SharePoint websites on SIPRNET. Data and information can be transferred using these platforms. Alternate methods are highly encouraged by using these mediums to avoid relying on removable media devices.


14. Training. The AC/S G-6/S-6 can provide training on writing to removable media devices if required. However, because removable media (external hard drives and CD/DVD writers) are common in our society this policy can be implemented without mandating training on writing to removable media. If movement to a non-US secret level system is required, use the data transfer procedures provided in the CLEAR training/tool located at: <https://dodiisclear.dia.mil/MainPage.htm>.

15. Administration/Inspection. A record of all removable media data transfers on classified system will be retained for at least five years. Commands will report by email to their respective I MEF or MSC Information Assurance Managers (IAM) at

Subj: PROCEDURES FOR TRANSFERRING INFORMATION TO CLASSIFIED
REMOVABLE MEDIA

the end of every calendar month, how many documents were transferred using removable classified media by each command. I MEF, MSC, local Security Managers and Information Assurance managers will randomly inspect commands every 30 days to ensure compliance.

16. Point of Contact. Contact the Command Information Assurance Management Office (IAM) or local Security Manager for further guidance.


G. M. RYAN
Chief of Staff

DISTRIBUTION LIST: I, II