



UNITED STATES MARINE CORPS  
MARINE CORPS INSTALLATIONS EAST  
PSC BOX 20005  
CAMP LEJEUNE NC 28542-0005

IN REPLY REFER TO:  
5239  
G-6  
03 APR 2012

COMMANDING GENERAL'S POLICY LETTER 004-12

From: Commanding General  
To: All Commanders, Marine Corps Installations East  
Subj: REMOVABLE STORAGE DEVICES

Ref: (a) DOD 5500.7-R, "Joint Ethics Regulation," March 25, 1996  
(b) CJCSI 6211.02C, DISN: Policy and Responsibilities, Jul 08  
(c) MCO 5239.2, Marine Corps Information Assurance Program (MCIAP)  
(d) MC EIAD OPSTD 005, Personal Electronic Devices (PEDs), Aug 03  
(e) MC EIAD OPSTD 011, Personally Identifiable Information, Apr 09  
(f) MC EIAD OPSTD 010, Unauthorized Disclosure and Electronic Spillage Handling, Sep 06  
(g) MARADMIN 647/08 of 18 Nov 08, Immediate Discontinued Use of Removable Media Storage and Memory Devices on Marine Corps Networks  
(h) Uniform Code of Military Justice  
(i) Department of Navy Civilian Human Resources Manual  
(j) MARADMIN 641/11 of 27 Oct 11, Marine Corps Blackberry Camera and Video Camera Waiver Process to use Camera and Video Features on Government Issued Blackberry

1. Purpose. This policy sets regulations and guidelines on the use of removable storage devices for all subordinate commands and personnel within Marine Corps Installations East (MCIEAST) area of responsibility (AOR), in accordance with references (a) through (j). This policy ensures MCIEAST personnel understand the importance of the proper usage of removable storage devices on the MCIEAST's computing enclaves. Additionally, this policy facilitates the prevention and detection of fraud, waste, and abuse as it relates to removable storage devices.

2. Background. Despite the operational necessity of removable storage devices, these beneficial devices pose risks to MCIEAST networks. The risks range from the unauthorized disclosure of unclassified information to the exfiltration of classified information to our combatant enemies. Per the references, MCIEAST will ensure technical and procedural controls are in place to reduce these risks, while ensuring that operational requirements can be met.

3. Scope. This policy applies to all MCIEAST Commands. Additionally, this policy applies to all service members, contractors, civilians, and foreign nationals utilizing any MCIEAST computing enclaves.

Subj: REMOVABLE STORAGE DEVICES

#### 4. Policy

##### a. Definitions

(1) MCIEAST computing enclaves, also referred to as "networks" in this policy, include any classified or unclassified networks for which MCIEAST has operational responsibility. These networks include, but are not limited to, the Secret Internet Protocol Router Network (SIPRNET), Non-secure Internet Protocol Router Network (NIPRNET), and Combined Enterprise Regional Information Exchange System (CENTRIXS)-International Security Assistance Forces (ISAF) (CX-I) network.

(2) Removable storage device refers to any information storage medium that can be attached to, inserted in, plugged into, or otherwise connected to a computer system to store, transmit, or process information/data. These devices are also referred to as removable secondary storage devices. Removable storage devices include, but are not limited to, thumb drives, memory sticks, flash drives, Universal Serial Bus (USB) drives, pen drives, external hard drives, phones, Personal Digital Assistants (PDA), personal computer memory card international association (PCMCIA) media, iPod and MP3 players, digital e-readers, floppy disks, external compact disks (CD) and digital video disk (DVD) burners (optical recording devices), and all other flash based storage devices.

(3) Flash media is defined as any solid state storage device and includes, but is not limited to, USB thumb drives, memory sticks/cards, or camera flash cards.

(4) For the purpose of this policy, government owned/procured devices are defined as those devices that have been purchased by a Department of Defense (DoD) agency for official use. This includes, but is not limited to, devices purchased by MCIEAST headquarters and subordinate commands.

(5) For the purpose of this policy, personally owned/procured devices are defined as those devices that have been purchased by an individual. Contractor owned/procured storage devices are defined in this category, and are not authorized for use unless explicitly authorized on a case-by-case basis by the Designated Approving Authority (DAA).

(6) Standalone computer systems are defined as machines/hosts that are not logically or physically connected to the MCIEAST networks at any time. These machines must be wiped and reimaged before being introduced back to MCIEAST networks.

##### b. General Policy

(1) This policy applies to any removable storage device that can be connected to a computing device via cable, USB, Firewire (IEEE 1394), PCMCIA, External Serial ATA, wireless, Bluetooth, infrared, and/or radio frequency. The purpose of the connection could be to

Subj: REMOVABLE STORAGE DEVICES

provide power, store, transmit, download, and/or upload data.

(2) The use of removable storage devices on MCIEAST networks will be limited to personnel who have an operational requirement to use the device. Where this requirement applies, commands will make every effort to provide government owned/procured products.

(3) The use of removable storage devices with the capability and/or technology to connect to computer systems via wireless, Bluetooth, 3-G, infrared, and/or radio frequency, is not authorized for use on MCIEAST computing enclaves at any time.

(4) The following guidelines apply for approval of removable storage devices for use on the MCIEAST computing enclaves:

(a) Approval may be granted for external USB hard drives containing spinning platters of any capacity.

(b) Use of RIM Blackberry devices on the network must comply with reference (j).

(c) All devices will be scanned, inspected, and approved by the local Cyber Security (CS) staff before being connected to the network.

(d) File security on the device must provide the same level of discretionary access control (DAC) as found on the computer to which it will connect (e.g. NTFS to NTFS). Authentication shall be active and used at all times.

(5) Personally owned/procured removable storage devices are not authorized for use on any MCIEAST network or standalone computer system.

(6) The following removable storage devices are not approved for use on MCIEAST network computer systems iPod or any type of MP3 Player, flash media/memory, USB thumb drives, digital e-readers, PCMCIA memory, PDA, cameras, or solid state drives in accordance with reference (g).

(7) In some instances (e.g., public affairs, combat correspondents, and intelligence), flash media is essential for performance of duties. If flash media/memory is essential for performance of duties, the transfer of data will be conducted from a standalone system to a CD-R or DVD-R.

(8) All removable storage devices connecting to MCIEAST classified networks (e.g., SIPRNET or CX-I) shall be treated as controlled items and handled according to local command physical security policy.

(9) All personally identifiable information (PII) stored on a removable storage device will be encrypted, per reference (e).

Subj: REMOVABLE STORAGE DEVICES

(10) Organizations issuing removable storage devices for official use shall control them in a manner consistent with accountability of other highly pilferable items.

(11) Removable storage devices involved in or affected by an electronic spillage, unauthorized disclosure, or breach of PII will be surrendered to the command's Security Manager and/or local CS staff immediately.

c. Usage Policy. The use of removable storage devices will be in accordance with DoD standards contained in the references. Removable storage devices introduced or connected to MCIEAST networks will be used for official business only. Removable storage devices will be used only for the transfer, transmittal, storage, or processing of DoD approved software and files. The use of removable storage devices for any other purpose(s) is not authorized.

(1) Exceptions to Policy. The MCIEAST Assistant Chief of Staff, G-6 (AC/S G-6) has final authority when approving exceptions to this policy. Exceptions to this policy will be considered based on mission necessity, adverse impact to CS, reliability, efficiency, and in accordance with DoD, United States Marine Corps, and local policies and regulations.

(2) Punitive Nature. This policy is punitive in nature; service members' failure to comply may result in administrative and/or punitive action, pursuant to Article 92 of reference (h). Civilian employees who fail to comply with this policy may receive corrective, disciplinary, and/or adverse action per reference (i).

d. Approval Request Procedures

(1) Personnel requesting the use of removable storage devices on the MCIEAST computing enclaves must read and understand this policy letter.

(2) All requests for use of removable media on MCIEAST networks will be routed in writing to the applicable CS section for approval.

(a) Requests must have respective cognizant section or unit AC/S or S-6 approval and justification prior to submission for final approval; and

(b) Request forms can be found on the MCIEAST G-6 CS SharePoint portal: (<https://intranet.mcieast.usmc.mil/G6/Cyber/Pages/default.aspx>) or by contacting the point of contact at paragraph 7 below.

(3) Local command CS staff shall complete the following tasks before approval:

Subj: REMOVABLE STORAGE DEVICES

(a) audit and remove any unauthorized software or files from the device;

(b) perform an up-to-date virus scan of all information contained on the device;

(c) ensure the storage device is formatted in NTFS; and

(d) ensure the appropriate classification label is affixed to the device.

e. Responsibilities

(1) The MCIEAST AC/S G-6 shall:

(a) ensure USB ports and PCMCIA port are disabled on computing devices that process classified material to the maximum extent possible; and

(b) serve as final approving authority for the introduction or use of removable storage devices except as noted in paragraph 4.a.(5) above.

(2) MCIEAST Commanders shall:

(a) ensure all members of the command are aware of the policies and prohibitions set forth in this policy;

(b) ensure command compliance with the standards outlined in this policy; and

(c) ensure procedures are established and practiced to ensure that government information is not exposed to unauthorized access or disclosure.

(3) Local CS staffs shall:

(a) serve as approving authority for the introduction or use of removable storage devices within their AOR;

(b) audit the use of removable storage devices on the MCIEAST networks within your AOR; and

(c) maintain a record of all approved devices.

(4) Users shall:

(a) maintain strict conformance to the standards and guidelines set forth in this policy;

(b) safeguard the information contained on the removable storage device from unauthorized or inadvertent modification, disclosure, destruction, or use; and

Subj: REMOVABLE STORAGE DEVICES

(c) report actual or potential security incidents, to include the possible loss or theft of any removable storage devices, associated with the use of MCIEAST computing systems to their local CS office regardless of the classification of its information content.

f. Handling and Destruction. Commands owning removable storage devices are responsible for destruction of those devices, per local command security policy.

#### 5. Classification and Marking

a. The connection of any removable storage device to a network makes the storage device permanently classified at the same level as the system to which it was connected. Any device introduced to classified computing systems can no longer be introduced into the computing devices of a lower classification. Contact your local command's Security Manager for declassification procedures and guidelines.

b. The removable storage device shall be classified at the highest level of data/information contained on the device. It shall be labeled with the highest overall classification level using the labels:

- (1) SECRET - Standard Form (SF) 707
- (2) SECRET/ISAF - CC FORM 16, June 09
- (3) CONFIDENTIAL - SF 708
- (4) UNCLASSIFIED - SF 710

c. When standard forms are not feasible due to interference with operation of the device, size of the media, etc., other means of marking may be used as long as they appropriately convey the classification and other required markings. For instance, a card can be attached to the device with the appropriate label affixed to the card or the device will be marked with a permanent marker indicating its classification level.

#### 6. Incident Response and Reporting

a. Electronic spillage, unauthorized disclosure, and/or breach or loss of PII will be immediately reported to the local command's Security Manager or CS Staff.

b. When responding to an incident, local commands will follow the procedures described in references (d) through (f).

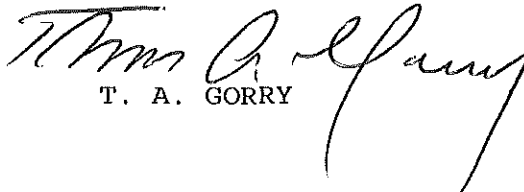
c. The reporting chain for responding to an incident is as follows:

- (1) Local Command CS Staff

Subj: REMOVABLE STORAGE DEVICES

- (2) Local Command Security Manager (classified only)
- (3) Local Command Special Security Office (SSO) (if spillage involves Sensitive Compartmented Information (SCI))
- (4) MCIEAST CS Manager
- (5) MCIEAST AC/S G-6
- (6) External Agencies

7. Point of contact for this policy is the MCIEAST G-6 CS Manager at DSN: 751-7050 or Comm: (910) 451-7050.

  
T. A. GORRY

Copy to:  
Security Manager