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

5239
G-6/CSD

19 FEB 2021

COMMANDING GENERAL'S POLICY LETTER 02-21

From: Commanding General
To: Distribution List

Subj: REMOVABLE STORAGE DEVICES

Ref: (a) DoD 5500.07-R Ch 7, "Joint Ethics Regulation (JER)," August 30, 1993
(b) CJCSI 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," January 24, 2012
(c) MCO 5239.2B
(d) USMC ECSM 005, "Portable Electronic Devices and Wireless Local Area Network Technologies," July 1, 2016
(e) USMC ECSM 011, "Personally Identifiable Information (PII)," April 30, 2013
(f) USMC ECSM 010, "Unauthorized Disclosure of Classified Information and Electronic Spillage," June 10, 2014
(g) USMC ECSM 008, "Cross Domain Solutions (CDS) and Secure Data Transfer (SDT)," February 15, 2019
(h) UCMJ
(i) DON Civilian Human Resources Manual
(j) MARADMIN 641/11
(k) DoDM 5200.01 Vol 2, Ch 3, "DoD Information Security Program: Marking Of Information," February 24, 2012
(l) DON CIO Memo, "Acceptable Use of DON Information Technology," February 12, 2016
(m) USMC ECSM 001, "Computer Security Incident Handling," August 8, 2012
(n) MARADMIN 590/05
(o) MARADMIN 732/07
(p) MCEN MSG 004-17, "Commercial Mobile Device (CMD) Guidance," August 3, 2017
(q) MCEN MSG 004-19, "Marine Corps Enterprise Network (MCEN) Computer Systems Planning Guidance for Microsoft Products"

Encl: (1) Removable Media Authorization and User Agreement
(2) Definitions

1. Purpose. To issue policy governing the use of external storage devices for all commands and personnel within Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ), in accordance with references (a) through (q). This policy ensures personnel understand the importance of the proper usage of removable storage devices on the Marine Corps Enterprise Network (MCEN) and stand-alone systems.

2. Cancellation. CG Policy Letter 010-19.

3. Background. Despite the operational benefits of removable storage devices, these devices pose significant risks to the MCEN, ranging from the

unauthorized disclosure of controlled unclassified information (CUI) to the exfiltration of classified information. Per references (a) through (q), MCIEAST will ensure technical and procedural controls are in place to reduce these risks, while making sure operational requirements can be met.

4. Scope. This policy applies to all MCIEAST Commanders. Additionally, this policy applies to all service members, contractors, civilians, and foreign nationals, accessing any MCEN or stand-alone computing systems within MCIEAST.

5. Policy

(a) General Policy

(1) This policy applies to any removable storage device capable of being connected to a computing system. A connection includes, but is not limited to, cable, universal serial bus (USB), FireWire (IEEE 1394), External Serial AT Attachment (eSATA), or wirelessly via infrared, Bluetooth, or Wi-Fi.

(2) The use of removable storage devices will be in accordance with Department of Defense (DoD) standards contained in references (a) through (q).

(3) The use of removable storage devices will be limited to personnel who have an operational requirement. Where this requirement applies, commands will provide government owned/procured devices.

(4) Removable storage devices introduced or connected to MCEN or stand-alone systems will be used for official business only; for the transfer, storage, or processing of DoD approved software and files. The use of removable storage devices for any other purpose is not authorized.

(5) Government owned Portable Electronic Devices will not be connected at any time to personally owned computer equipment (e.g. 'hot docking' between government and non-government owned computers).

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

(7) Removable storage devices with the capability and/or technology to connect to computer systems via wireless technology are not authorized for use on MCEN at any time.

(8) The following guidelines apply for approval of removable storage devices for use on MCEN:

(a) All external storage devices must be government owned and procured.

(b) All external storage devices must be inspected, registered, and approved by the local command G/S-6 before connection to the MCEN or stand-alone computing systems.

(c) Use of cellular devices on the MCEN must comply with reference (p).

(d) External storage devices must be scanned for malware and unauthorized software utilizing an enterprise approved version of anti-virus

software with latest virus definitions before connection to the MCEN is authorized.

(e) All removable storage media shall be labeled appropriately, per paragraph 6, indicating the classification level.

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

(9) All removable storage devices connecting to MCEN classified networks shall be treated as controlled items and handled according to local command security policy.

(10) All CUI, to include Personally Identifiable Information (PII) stored on a removable storage device will be encrypted, per reference (o).

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

(12) Removable storage devices involved in or affected by an electronic spillage, unauthorized disclosure, or breach of PII will be immediately surrendered to the command's Security Manager or Information System Security Manager (ISSM).

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

c. Approval Request Procedures

(1) Personnel requesting the use of removable storage devices on the MCEN must:

(a) Read and understand this policy letter;

(b) Complete enclosure (1) blocks 1-12a per the instructions; and

(c) Route enclosure (1) per the instructions until completed.

(2) All requests for use of removable media on MCEN will be submitted in writing to the local G/S-6 for approval utilizing enclosure (1).

(3) Local command cyber security staff or G/S-6 shall complete the following tasks before approval:

(a) The ISSM or Information Systems Security Officer (ISSO) will validate enclosure (1) and complete 14 series blocks per the instructions, forward via appropriate channels for action officer approval for use on classified enclave.

(b) All storage devices will be wiped prior to initial use or after loss of positive control.

(c) All storage devices will be formatted in NTFS and provided an appropriate Device Identification.

(d) Perform a full virus scan of device with current virus definitions for previously authorized and prepared removable media.

(e) Audit and remove any unauthorized software from the device.

(f) Ensure the appropriate classification label is affixed to the device.

(g) Maintain enclosure (1), for record of compliance in regards to monitoring in accordance with paragraph 5f(3)(b) and (c).

d. Data at Rest. Per reference (q), Bitlocker to Go is the designated solution for encryption of removable hard drives. Removable storage media is required to be encrypted, otherwise be "read only."

(1) If there is a requirement to exempt the use of Bitlocker to Go and maintain write access, an exemption must be requested.

(2) Unit G/S-6 sections and information system coordinator (ISC) will submit a Remedy request to the MCIEAST G-6 ISSM to be routed for approval by the USMC Authorizing Official.

e. Punitive Nature. This policy is punitive in nature; Service Members who fail to comply with this policy may receive administrative and/or punitive action, pursuant to Article 92 of reference (h). Civilian employees and contractors who fail to comply with this policy may receive corrective, disciplinary, and/or adverse action per reference (i). In addition to the above, the following actions will occur:

(1) First Offense: A notification will be sent to the offender and the offender's unit for action.

(2) Second Offense: A notification will be sent to the offender's unit. The offender will be required to complete remedial training as prescribed by MCIEAST-MCB CAMLEJ G-6 Cyber Security Division (CSD), complete a new System Authorization Access Request (SAAR) and forward all documentation to MCIEAST-MCB CAMLEJ G-6 CSD Cyber Incident Response Team (CIRT). The account will be disabled until documentation of remedial training and SAAR is received.

(3) Third Offense: A notification will be sent to the offender's unit. The offender will be required to complete remedial training as prescribed by MCIEAST-MCB CAMLEJ G-6 CSD. The offender must complete a new SAAR and forward all documentation to MCIEAST-MCB CAMLEJ G-6 CSD CIRT. The account will be disabled for up to three months, it will be enabled at the end of the suspension if the required documentation is received.

(4) Further offense(s) may result in account(s) being permanently disabled.

f. Responsibilities

(1) MCIEAST-MCB CAMLEJ AC/S, G-6 shall:

(a) Ensure USB ports are disabled on computing devices that process classified material to the maximum extent possible.

(b) Serve as final approving authority for exception to policy required for the use of removable storage devices as noted in paragraph 5b 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.

(c) Ensure procedures are established and practiced to make certain government information is not exposed to unauthorized access or disclosure.

(3) Local cybersecurity staffs shall:

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

(b) Audit the use of removable storage devices on the MCEN within their 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.

(c) Report actual or potential security incidents, to include the possible loss or theft of any removable storage devices, associated with use on MCEN to local cyber security regardless of the classification of its information content.

g. Handling and Destruction. Commands owning removable storage devices are responsible for appropriate handling and destruction of those devices, per the local command's security policy.

6. Classification and Marking

a. The connection of a removable storage device to a network makes the storage device permanently classified at the level of the system to which it was connected. Any device introduced to a classified computing system can no longer be introduced into any computing device of lower

classification. Contact your local command's Security Manager regarding control and 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 - SF 707;

(2) CONFIDENTIAL - SF 708;

(3) 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 example, 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.

7. Incident Response and Reporting

a. Electronic spillage, and unauthorized disclosure, will be immediately reported to the local command's Security Manager.

b. Breach or loss of PII will be reported to the local command's Privacy Act Coordinator.

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

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

(1) Local Command ISSM;

(2) Local Command Privacy Act Coordinator (PII breach);

(3) Local Command Security Manager (classified only);

(4) Local Command Special Security Office (if spillage involves Sensitive Compartmented Information);

(5) MCIEAST-MCB CAMLEJ ISSM;

(6) MCIEAST-MCB CAMLEJ AC/S, G-6; and

(7) External Agencies/Reporting.

8. Point of contact for this policy is the MCIEAST-MCB CAMLEJ G-6 ISSM at DSN: 751-7050 or Commercial: (910) 451-7050.

J.D. ALFORD

DISTRIBUTION: A/B/C

19 FEB 2021

Subj: REMOVABLE STORAGE DEVICES

UNCLASSIFIED//FOUO

UNITED STATES MARINE CORPS
REMOVABLE MEDIA AUTHORIZATION AND USER AGREEMENT

1. LAST NAME | 1-A. FIRST NAME, MIDDLE INITIAL | 2. RANK/RATE | 3. EDIPI | 4. START DATE | 4-A. END DATE

5. UIC | 5-A. PARENT COMMAND | 5-B. UNIT/SQUADRON | 5-C. SECTION/SHOP | 6. PHONE NUMBER

7. COMPUTER NAME | 7-A. MEDIA ACCESS CONTROL (MAC) ADDRESS | 8. CLASSIFICATION (ENCLAVE) ◯ Unclassified/NIPR ◯ Classified/SIPR | 8-A. CLEAR TRAINING COMPLETION DATE

9. EXTERNAL MEDIA DEVICE MAKE/MODEL/SIZE | 9-A. EXTERNAL MEDIA SERIAL NUMBERS | 9-B. FLASH / SOLID STATE MEDIA ◯ YES ◯ NO

10. JUSTIFICATION

11. USER AGREEMENT

- The purpose for the request is for mission essential purposes.
- I affirm that the listed removable media device is government procured, owned and controlled
- New devices will be wiped and formatted to National Technology File System prior to use on Marine Corps Enterprise Network (MCEN). Devices with existing data will be scanned on a stand-alone host.
- I understand the removable media listed in this agreement is only to be used on a Department of Defense (DoD) system of the same classification level and that I will adhere to references mentioned within this agreement.
- I am responsible for all actions regarding use of the removable media listed in this agreement.
- I will not use government owned removable media with personal or other unauthorized computers.
- I will not copy, store, transmit, access or transfer any unauthorized data or software onto the approved removable media or a DoD system connected to the MCEN-N, MCEN-S or coalition computing enclave.
- I will ONLY use CD-R, CD-R or DVD+R media during high to low and low to high transfers.
- I will not upload any higher classification data to any device that is marked of a lower classification.
- I will not air gap using media from higher to lower classification system unless I have been appointed as a Data Transfer Agent and the document has been approved for transfer by a Foreign Disclosure Officer (FDO) or Foreign Disclosure Representative (FDR) or Special Security Officer.
- I will power down volatile memory devices for 60 seconds before connecting to any device.
- I will contact a FDR, FDO, security manager or command cybersecurity (CY) section to assist with transfer of information from a higher to lower classification system.
- In the event of ANY violation/spillage I will immediately notify my command security manager and CY section.
- I understand that the external media device will be scanned by my local S-6 on a standalone system running current anti-virus and definitions BEFORE using it on a different DoD system.
- I will coordinate with the security manager for proper labeling and handling of external media.
- I understand that the device and information contained on this device is government owned and must be protected and will not be used or maintained on any personal system.
- I understand it is prohibited to disguise Universal Serial Bus drives.
- I will report lost or stolen external media to my security manager or CY section upon discovery.
- I will complete CLEAR training.

I have read, understand and will comply with the below and applicable references. Failure to do so will result in removal/denial of access and possible confiscation of external media:

- ECSM 005 Portable Electronic Devices and Wireless Local Area Network Technologies
- ECSM 008 Cross Domain Solutions and Secure Data Transfer
- MCO 5239.2B Marine Corps Cybersecurity
- MARADMIN 225/11 Update to protection of classified information on DoD Secret Internet Protocol Router Network (SIPRNET) networks
- USCYBERCOM CTO 10-133
- USCYBERCOM CTO 10-133A
- USCYBERCOM CTO 10-084
- USCYBERCOM CTO 10-084A

12. REQUESTOR SIGNATURE | 12-A. DATE

SUPERVISOR

13. RECOMMENDATION | APPROVED ☐ | DISAPPROVED ☐

13-A COMMENTS

13-B SUPERVISOR SIGNATURE | 13-A. DATE

COMMAND INFORMATION SYSTEM SECURITY MANAGER (ISSM) / OFFICER (ISSO)

14. RECOMMENDATION | APPROVED ☐ | DISAPPROVED ☐

14-A COMMENTS

14-B. COMMAND ISSM/ISSO SIGNATURE | 14-C. DATE

FLASH MEDIA NOT SUPPORTED ON CLASSIFIED ENCLAVES IN ACCORDANCE WITH US CYBER COMMAND COMMUNICATIONS TASKING ORDER

COMMAND SECURITY MANAGER

15. DECISION | APPROVED ☐ | DISAPPROVED ☐

15-A COMMENTS

15-B. SECURITY MANAGER SIGNATURE | 15-C. DATE

AUTHORIZING OFFICIAL (AO) / CERTIFYING AUTHORITY REPRESENTATIVE (CAR) / SECURITY CONTROL ASSESSOR REPRESENTATIVE (SCAR)

16. DECISION | APPROVED ☐ | DISAPPROVED ☐

16-A COMMENTS

16-B. APPROVING AUTHORITY SIGNATURE | 16-C. DATE

MCIEAST - MCB CAMLEJ/G-6/CSD/1 (REV 8/19) PREVIOUS EDITIONS ARE OBSOLETE LIVE CYCLE DESIGNER

Enclosure (1)

Subj: REMOVABLE STORAGE DEVICES

UNCLASSIFIED//FOUO
UNITED STATES MARINE CORPS
REMOVABLE MEDIA AUTHORIZATION AND USER AGREEMENT
INSTRUCTIONS

REQUESTOR INFORMATION

1. **LAST NAME**. The last name of the user.
1-A. **FIRST NAME, MIDDLE INITIAL**. The first name and middle initial of the user.
2. **RANK/RATE**. Rank and rate of the user.
3. **EDIPI**. 10 digit EDIPI of the user.
4. **START DATE**. Date requested to start use of external storage device. **Note: this date cannot be guaranteed and may take a week or more to process.**
4-A. **END DATE**. Last day access is needed. If for exercise purposes only annotate the last day of exercise. All exemptions require annual review at this date for continued usage.
5. **UIC**. Unit Identification Code of the users command.
5-A. **PARENT COMMAND**. Parent major command of the user. (II MEF, 2MLG, 2MAW, 2MarDiv)
5-B. **UNIT/SQUARDON**. Unit or squadron of the user. (MEF CE, CLR 35, MAG-26, 8th Marines)
5-C. **SECTION/SHOP**. Section or shop of the user (G-6, S-3, Armory)
6. **PHONE NUMBER**. Phone number by which the user can be contacted, annotate for DSN as applicable. (DSN 123-4567)
7. **COMPUTER NAME**. Fully qualified computer name for the requested use of external media. (NESTW13100L###.mcdsus.mcds.usmc.mil)
7-A. **MEDIA ACCESS CONTROL (MAC) ADDRESS**. The MAC address of the computer can be found using command prompt or PowerShell and typing in ipconfig /all.
8. **CLASSIFICATION (ENCLAVE)**. Select the enclave for which the device is being requested.
8-A. **CLEAR TRAINING COMPLETION DATE**. ONLY REQUIRED FOR CLASSIFIED ENCLAVES. Date of CLEAR training completion.
Training is available at: (NIPR) https://icclearn01.oni.nmci.navy.mil || (SIPR) https://icclearn01.oni.nmci.navy.smil.mil
   1. Click on the Training & Info button.
   2. Click on the CLEAR Tool Tutorial link.
   3. Click on Launch New CLEAR Tool Tutorial.
   4. Complete training and pass the test.
   5. Submit the training certificate with this completed form.
9- **EXTERNAL MEDIA DEVICE MAKE/MODEL/SIZE**. Annotate the external media make, model and size in Megabytes/Gigabytes requested.
9-A. **EXTERNAL MEDIA SERIAL NUMBERS**. Annotate the external media serial number(s).
9-B. **FLASH / SOLID SATE MEDIA**. Identify external media is/is not flash or solid state memory.
10. **JUSTIFICATION**. Describe why information cannot be kept within the respective computer or transferred using means such as posting on SharePoint, retyping, etc. Include the following information:
   - What type of information will be transferred and in what format (Email, Power Point, Graphics, Imagery, etc.).
   - How often will external media be accessed?
   - What alternatives have you investigated, and why can alternatives not be utilized?
   - How will the function or task be impacted if this request is not approved?
11. **USER AGREEMENT**. Acknowledgment of responsibilities. Before digitally signing block 12, the user must understand the data transfer procedures.
12. **REQUESTOR SIGNATURE**. Digitally sign this block using your DoD issued Public Key Infrastructure (PKI) certificate.
12-A. **DATE**. Date requestor digitally signed the request.

SUPERVISOR APPROVAL (Commanding Officer, Executive Officer, Assistant Chief of Staff or Equivalent Endorsement)

13. **RECOMENDATION**. Determine the necessity of the request in order to assist the section with transferring essential data; select the appropriate box. Supervisors must understand the risk of possible unauthorized classified information dissemination.
13-A. **COMMENTS**. If approval is not recommended, suggest or direct alternative methods.
13-B. **SUPERVISOR SIGNATURE**. Digitally sign this block using your DoD issued PKI certificate.
13-C. **DATE**. Date supervisor digitally signed the request.

COMMAND ISSM/ISSO

14. **RECOMENDATION**. The unit ISSM/ISSO will confirm that:
   Other, more secure means of information transfer are not viable.
   Only a minimum number of people and a minimum number of computers will be authorized to use external media.
14-A. **COMMENTS**. If approval is not recommended, suggest alternative methods. ISSO must provide the Electronic Identifier. This is the unique number used to identify the specific external media. To locate the ID# of the requested external media, the media must be connected to a stand alone computer. Once connected go to Device Manager and expand disk drives. View properties on the external hard drive and go to the Details tab. From the Property drop down box, select Device Instance Path to obtain the value.
14-B. **COMMAND ISSM/ISSO SIGNATURE**. Digitally sign this block using your DoD issued PKI certificate.
14-C. **DATE**. Date ISSM/ISSO digitally signed the request.

(CLASSIFIED ENCLAVE USE ONLY)

UNIT SECURITY MANAGER

15. **DECISION**. Recommend approval if the requestor's security access and security training are current, and procedures are in place to adequately control classified information derived from the classified networks. The Security Manager and/or their staff have verified that the requestor has completed the **Data Transfer Training CLEAR**.
15-A. **COMMENTS**. Use this block if approval is not recommended.
15-B. **SECURITY MANAGER SIGNATURE**. Digitally sign this block using your DoD issued PKI certificate.
15-C. **DATE**. Date Security Manager digitally signed.

AO/SCAR

16. **DECISION**. Review risk and document approval/disapproval decision based on recommendations.
16-A. **COMMENTS**. Information regarding the decision and acknowledgment of risk accepted.
16-B. **APPROVING AUTHORITY SIGNATURE**. Digitally sign this block using your DoD issued PKI certificate.
16-C. **DATE**. Date AO/CAR/SCAR digitally signed the request

MCIEAST - MCB CAMLEJ/G-6/CSD/1 (REV 8/19) PREVIOUS EDITIONS ARE OBSOLETE LIVE CYCLE DESIGNER

Subj: REMOVABLE STORAGE DEVICES

DEFINITIONS

MCIEAST Computing Enclaves: Referred to as "networks," 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), and Non-secure Internet Protocol Router Network (NIPRNET).

Removable Storage Device: 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, USB drives, pen drives, external hard disk drives, phones, personal digital assistants, PCMCIA media, iPod and MP3 players, digital e-readers, smartwatches, external compact disk and digital video disk burners (optical recording devices), and all other flash based storage devices.

Flash Media: Includes, but is not limited to, solid state drives, USB thumb drives, memory sticks/cards, and camera flash cards.

Government Owned/Procured Devices: For the purpose of this policy, are defined as those devices that have been appropriately purchased by a DoD agency for official use.

Personally Owned/ Procured Devices and Contractor Ownwed/Procured Devices: For the purpose of this policy, are defined as those devices that have been purchased by contracting company. These devices are not authorized for use unless explicitly authorized on a case-by-case basis by the Major Subordinate Command ISSM.

Stand-Alone Computer: A computer system that does not logically or physically connect to the MCEN at any time. Stand-alone computers will meet all Information Assurance Vulnerability Alert, Security Technical Implementation Guideline, Host Based Security System and Anti-virus compliance. A stand-alone computer will be used to scan authorized external media for malicious and unauthorized software, prior to the media being introduced to the network.

Wireless Connection: Any connection between two devices where there is no physically wired connection. Wireless connections include but are not limited to, 802.11X, Bluetooth, 3-G, 4-G, infrared, and/or other radio frequency.