



DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS MARYLAND 21402-1300

USNAINST 8510.02A
28/ITSD
12 Sep 2016

USNA INSTRUCTION 8510.02A

From: Superintendent, U.S. Naval Academy

Subj: GOVERNMENT-ISSUED COMMERCIAL MOBILE DEVICE

Ref: (a) USNAINST 8510.01, Cybersecurity Risk Management
(b) USNAINST 7320.10, USNA Management of Personal Property
(c) OPNAVINST 2100.2A, Navy Policy and Procedures on the Issuance, Use, and Management of Government-Owned Cellular Phones, Personal Digital Assistants, and Calling Cards

Encl: (1) Mobile Device Use Agreement

1. Purpose. Per reference (a), this instruction establishes U.S. Naval Academy (USNA) policy for configuring and using a government-purchased Commercial Mobile Device (CMD).
2. Cancellation. USNAINST 8510.02 dated 26 Apr 2016.
3. Scope and Applicability. This instruction applies to government-purchased smartphones and tablet computers that are issued into the custody of certain USNA staff members. This instruction does not apply to laptop computers.
4. Background. CMDs are issued to facilitate email, text, voice, and video communications supporting timely, responsive, and efficient duty performance for a small number of USNA staff employees in unique positions. They are not issued for recreation or personal social media purposes. The small size and mobility inherent in CMDs present a unique risk to information security and highly portable devices such as smartphones and tablets that can easily be misplaced, forgotten, or stolen, present an even greater risk. Proper device configuration and safe operational behavior provide defense against these risks. CMDs purchased by USNA for issue are not configured to use Public Key Infrastructure (PKI) and therefore have additional use restrictions.
5. Policy. Requirements and guidelines to properly configure and use CMDs are specified in the following areas: general policies and operational behavior; email, messaging, and web browsing; applications; connections; multimedia; and enterprise configuration management.

a. General Policies and Operational Behavior

(1) CMDs shall be reset to factory default settings before re-configuring it for issue to a new user.

(2) CMD may only be issued to a specific USNA employee for their individual use only, and may not be loaned to another individual. An exception may be authorized by the Information Technology (IT) Services Division (ITSD) Deputy for Information Technology/Chief Information Officer for a mobile device configured with an authorized group account (e.g., Naval Academy Duty Officer).

(3) Before the first use of a CMD, an employee must complete the prescribed CMD training and digitally sign a Mobile Device User Agreement. CMD users must subsequently complete the prescribed annual training on using the device and security.

(4) The USNA Acceptable Use Policy for USNA IT Resources and the Navy User Agreement apply to using a CMD.

(5) Except in an emergency, a CMD shall not be used while driving unless used in a hands-free manner where such use is not prohibited by DoD or state law.

(6) Users shall not transmit or receive classified information by any means when using a CMD (e.g., email, text, voice, or image) or process or store classified information on a CMD. CMDs are not permitted in any location where classified documents or information are stored, transmitted, or processed.

(7) Physical control shall be maintained at all times. CMDs shall not be left unlocked or unattended in public places. Personnel shall be cognizant of the physical environment if a CMD is used to discuss sensitive information.

(8) Location services shall be turned off when not in use.

(9) Users shall not attempt to circumvent security ("hack," "jailbreak," or "root").

(10) A CMD user must notify ITSD prior to relocating the CMDs outside the United States and obtain prior approval to use international cellular service. A user will be held responsible for international roaming charges if charges were not authorized in advance. WiFi will be disabled on CMDs that are relocated outside of the United States. The CMD user must contact ITSD upon returning to the United States to have the CMD wiped and reconfigured.

(11) A CMD user has stewardship responsibility for prudent voice and data usage. A CMD should not be used for voice communication when a landline is available (e.g., in the user's office), nor should the CMD be used to access internet services when a government computer

can be used. Except when actively in use, the CMD should remain off in areas subject to roaming charges.

(12) Voice and text messaging used for a non-official purpose is permitted only if the use occurs on breaks, lunch periods, or non-duty hours; does not adversely affect the employee's performance or accomplishing the USNA mission; does not reflect adversely on USNA, DON, DoD, or the U.S. Government; and does not incur additional cost to the U.S. Government.

b. Applications. The following policy pertains to application installation, use, and removal:

(1) The USNA Configuration Control Board (CCB) shall conduct a risk assessment and approve all applications and application updates, including over-the-air updates, prior to installing the work profile.

(2) When available, firewall and antivirus solutions shall be installed and kept up-to-date on CMDs. Users shall not attempt to disable or otherwise change firewall and antivirus configuration settings.

c. Email, messaging, and web browsing:

(1) The enterprise email service accessed from the enterprise-managed profile shall be used for all work related email communication. A personal email account accessible from a personal profile shall never be used for work related email communication.

(2) Email sent from a CMD shall not disclose that the email originated from a mobile device (e.g., "Sent From My Smartphone").

d. Connections

(1) Cellular. CMDs shall only connect to the USNA-approved cellular carrier. Users shall not attempt to "unlock" or otherwise modify a device to change carriers.

(2) WiFi. A WiFi capable CMD:

(a) Is never permitted to connect to:

1. A classified wireless network (e.g., Non-Secure Internet Protocol Router Network and Secret Internet Protocol Router Network).

2. A WiFi network outside of the United States.

(b) Is permitted to connect to:

1. The unclassified wireless USNA mission network for non-privileged access only.

2. A home wireless network ONLY if an enterprise-managed "work profile" is configured on the device.

3. A public WiFi network.

4. A hotel WiFi network.

(c) Must not broadcast WiFi as an access point (i.e., function as a router for a wireless network). WiFi shall be disabled when not in use.

(d) Must be configured, as possible, to prompt users before connecting to a wireless network.

(3) Bluetooth. Bluetooth use is prohibited except when a CMD is connected for hands-free voice communication. At all other times Bluetooth shall be disabled.

(4) USB and storage. USB connections are prohibited. A CMD shall not be used as a removable storage device, and a removable storage device (e.g., USB flash drive, external hard drive, Secure Digital (SD) flash card) may not be connected to a CMD.

e. Multimedia. CMDs are issued to facilitate work-related email, text, and voice communications. The following policies pertain to using and storing multimedia (audio, video, pictures, and streamed content) on CMDs:

(1) Using removable media such as SD cards is not permitted.

(2) Screen capture shall not be used.

f. Enterprise Management. CMDs will be managed on a USNA enterprise basis as a separate collection of devices with security policies that differ from personally owned portable electronic devices:

(1) The most recent version of the CMD Operating System (OS) shall be present on the device.

(2) CMD security configurations shall not be changed by the user.

(3) The most recent version of a Device Policy Application, if available, shall be installed and functioning. The following minimum set of settings shall be enforced if supported by the CMD OS:

(a) The device must be registered with the USNA enterprise CMD management system.

- (b) Data on the CMD is encrypted.
- (c) Application auditing is enabled.
- (d) Remote wipe by user is enabled.
- (e) CMD sync to the USNA domain is enabled.
- (f) A PIN, password, or passcode of at least eight characters must be set.
- (g) The screen will lock after no more than five minutes of inactivity.
- (h) Data on the CMD will be wiped after 10 unsuccessful password attempts.
- (i) Data on the CMD will be wiped automatically after 35 days of inactivity.
- (j) CMDs will be blocked upon detecting installation of a superuser binary.

6. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV Manual 5210.1 of January 2012.

7. Review and Effective Date. Per OPNAVINST 5215.17A, ITSD 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.


W. E. CARTER, JR

Releasability and Distribution:
Non Mids (electronically)

GOVERNMENT-ISSUED COMMERCIAL MOBILE DEVICE USE AGREEMENT

A Government-issued Commercial Mobile Device (CMD) is issued to facilitate email, text, voice, and communications for official business associated with assigned duties.

1. CMDs are for unclassified use only, will not be taken into an area where classified information is processed, and will not be connected to a classified network or information system. Classified or sensitive information shall not be discussed on a CMD.
2. I will act as a responsible steward of voice and data charges. Charges associated with unauthorized use will be paid by the user.
3. I will immediately notify my supervisor and the USNA Information System Security Manager (ISSM) if a CMD or calling card is lost, stolen, or damaged. I will reimburse the government to replace a CMD that is lost due to my negligence.
4. I will immediately notify my supervisor and the USNA ISSM if a data spill occurs.
5. I will keep location services and the Bluetooth and WiFi radios off at all times except when required for use.
6. I will not take a CMD overseas unless granted prior approval by ITSD.
7. I understand that in addition to administrative and disciplinary action, improper use may result in a revocation of my device or calling card use.
8. I have read, understand, and will comply with the Government-Issued Commercial Mobile Device Policy, the USNA Acceptable Use Policy for Information Technology Resources, and the Navy User Agreement and Notice and Consent Provisions.
9. Signing this agreement documents your consent to the provisions above, that you acknowledge the device is for authorized use only, and that you acknowledge receipt and assume custodial responsibility for the following items:

Make and Model: _____
Serial Number: _____
Service Provider: _____
Digital Signature: _____