



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:

5500

ARS

10 NOV 2015

Security Note 08-15

From: Director, Administration and Resource Management Division
To: Security Coordinators

Subj: GUIDANCE ON THE PROPER USE OF DOD MOBILITY CLASSIFIED
CAPABILITY-SECRET (DMCC-S) DEVICE AND OTHER AUTHORIZED
CLASSIFIED PORTABLE ELECTRONIC DEVICE (PED)

Ref: (a) Secretary of Defense Memo Security and Operational Guidance for Classified
Portable Device dated 25 September, 2015
(b) OPNAVISNT C5510.93F/MCO 5510.19, Navy/Marine Corps Implementation of
National Policy on Control of Compromising Emanations
(c) Department of Defense DMCC-S User Agreement

1. **Introduction.** In accordance with the references, the following guidance shall be adhered to when using the DoD Mobility Classified Capability-Secret (DMCC-S) device and other Portable Electronic Devices (PED) capable of sending/receiving audio and observable classified data (i.e., Secure iPad, tablets, IRIDIUM phones in "secure mode", portable SIPRNET printers, or SIPRNET laptops) in areas designated **unsafe** for exploitation of compromising emanations (CE). According to reference (a), a classified PED is one that has been verified as compliant with National Security Agency (NSA) requirements for processing classified information, including but not limited to tablets, laptops, smartphones, and cellular telephones. Only cleared, trained, and authorized DoD personnel, contractors, and/or DoD mission partners shall operate and manage classified PEDs. Authorized personnel must possess a security clearance that is equal to or higher than the information being accessed and transmitted. Personnel who are authorized to use a DMCC-S or other type of PEDs are required to sign a user agreement indicating that they understand classified PED handling and security requirements as outlined in the user agreement, user manual, and this security note.

2. **Background.** In accordance with reference (b), the existence and study of the nature of CE are referred to as TEMPEST. TEMPEST is a code word used to describe the unintentional data-related or intelligence-bearing signals. If these signals are intercepted and analyzed, they could disclose the information transmitted, received, handled, or otherwise processed by electrical information-processing equipment or systems. Any type of electrical information-processing device, whether an ordinary electrical typewriter or a large complex data processor, may produce CE. Although comprehensive national threat evaluations are performed on a continuing basis to identify the nature and extent of the TEMPEST threat, foreign governments are actively engaged in attacks against U.S. secure communications and other information-processing facilities for the expressed intention of exploiting CE.

Subj: GUIDANCE ON THE PROPER USE OF DOD MOBILITY CLASSIFIED
CAPABILITY-SECRET (DMCC-S) DEVICE AND OTHER AUTHORIZED
CLASSIFIED PORTABLE ELECTRONIC DEVICE (PED)

3. Usage. The DMCC-S and other secure PEDs allow authorized cleared personnel mobility and accessibility to classified information. Users must be aware of the threat and vulnerability factors that are present. It is the user's responsibility to maintain situational awareness of their surroundings and practice OPSEC procedures. If the device is being used in "classified mode", users shall maintain an awareness of their surroundings and proximity to uncleared personnel. All PEDs including the DMCC-S shall not be marked with an external/visible classification label, so as to attract undue attention to the device or the authorized user. This document will provide guidance on the processing, conversing, reading, or viewing of National Security Information in public and private spaces (i.e., hotel conference room or any other location not approved to store or transmit classified information).

4. Safeguarding. All users shall protect DMCC-S and other PEDs such as Secure iPads, tablets, IRIDIUM phones in "secure mode" and portable SIPRNET printers, and SIPRNET laptops based on the level of classification. When required to use the device, individuals should isolate themselves from the general public and ensure sufficient privacy is available to allow the equipment to be used in "classified mode" with minimal risk. Users are reminded to be continuously observant of their surroundings when using classified mobile devices. Users must maintain continuous physical control of the device in a manner that will minimize the possibility of loss, theft, unauthorized use, or tampering. Users shall inspect the device for signs of tampering. Attempting to open any part of the device is strictly prohibited.

5. Traveling. Users are not required to carry a courier card/letter with the classified PED. When possible, any WiFi, NFC, or Bluetooth capabilities must be disabled or deactivated by the user. Secure PEDs and DMCC-S shall be placed in "airplane mode" and powered down prior to going through an inspection point. All classified PEDs may be x-rayed or physically/visually inspected at installation entry points, airports, and other similar locations where such devices are routinely inspected, as long as the device remains within the user's line of sight. During flight, the device should remain powered down or in "airplane mode".

6. Storage. DMCC-S and other Secure PEDs shall be stored in a GSA approved container and spaces approved for their storage unless material or devices are under the direct sight and control of authorized persons. When traveling outside the National Capital Region, to foreign countries, or areas where threat levels are elevated and pose higher risks to enemy exploitation activities, it is imperative to have two couriers and to plan ahead by contacting and utilizing available U.S. embassies or U.S. military-controlled installations to store and process classified information, material, and/or equipment. Storing secure PEDs inside a safe at a hotel is strictly prohibited unless the user is in the room. At no time will a user leave the hotel room without the secure PED even when it is stored inside a safe. Hotel employees have the capability to access the safe without knowing the combination settings that have been set for the safe. Users must maintain positive control of the device during business travel at all times.

Subj: GUIDANCE ON THE PROPER USE OF DOD MOBILITY CLASSIFIED
CAPABILITY-SECRET (DMCC-S) DEVICE AND OTHER AUTHORIZED
CLASSIFIED PORTABLE ELECTRONIC DEVICE (PED)

7. Reporting. Report all lost, damaged, or improperly destroyed devices to the Security Manager and Defense Information System Agency Customer Contact Center at DSN 312-770-9500 or Toll Free 1-855-868-9500.

8. This supersedes Security Note 06-11.

9. Questions regarding this Security Note should be directed to Mr. Isaac Encarnacion at 703-614-2305 or email: isaac.encarnacion@usmc.mil.


J/R. NEWELL
By direction

Copy to:
ARS
File