DEPARTMENT OF THE ARMY
U.S. ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT DETRICK
810 SCHREIDER STREET, SUITE 212
FORT DETRICK, MARYLAND 21702-5000

IMFD-PL

OCT 0 2 2017

MEMORANDUM FOR All U.S. Army Garrison Fort Detrick Personnel

SUBJECT: U.S. Army Garrison Policy Memorandum # 11, Policy on Personal or Governement Electronic Devices

1. References.

a. Department of Defense Directive (DoDD) 5205.02E (DoD Operations Security (OPSEC) Program), 20 June 2012.

b. DoD Manual 5205.02-M (DoD Operations Security (OPSEC) Program Manual), 03 November 2008.

c. DoD Memorandum, Introduction and Use of Wearable Fitness Devices and Headphones within DoD Accredited Spaces and Facilities, 21 April 2016.

d. HQDA EXORD 018-17, Restricting Personal Electronic Devices (PEDs) at Training/Briefing Sessions in Order to Mitigate Vulnerabilities and Reduce OPSEC Violations, 28 October 2016.

e. HQDA EXORD 042-17, Personal Electronic Devices (PED) Level Designation Standardization at Training/Briefing Sessions in Order to Mitigate Vulnerabilities in Cyberspace, 06 August 2017.

f. Army Regulation 530-1 (Operations Security), 13 October 2014.

2. The purpose of this policy is to establish U.S. Army Garrison's policy and procedures governing Personal Electronic Devices (PEDs) at official meetings and events. PEDs are defined as personal devices that communicate, send, receive, store, reproduce, or display voice or text communication data to include cell phones, laptops, fitness trackers, and cameras. Government issued devices are included in this list (e.g. Blackberries, iPads, iPhones, smart wrist watch phones, and wireless headphones at a minimum). This list is not all inclusive.

3. This policy is effective for all personnel assigned, attached, or under the operational control of U.S. Army Garrison. The policy for personal and government mobile devices, as outlined in this memorandum, will ensure U.S. Army Garrison personnel maintain OPSEC measures and eliminate unnessasary release of sensitive information via these devices. The intent of this policy is to enhance operational security during operations, training, exercises, meetings, and briefings.

4. Garrison Soldiers and Civilians who violate these prohibitions may be subject to appropriate disciplinary, administrative, or other action as applicable.

5. The following PED levels will be designated for all USAG military training events, briefings, meetings and operations. The PED level will be annotated on the training schedule so all are aware of what is allowed. PED levels will be prominently displayed at the entrance to each location that falls within the USAG and explained by the briefer, instructor, or person in charge in advance of any event. There are three distinct PED categories:

a. PED 0 = No PEDs allowed – This category is reserved for USAG events at which classified or sensitive information is discussed or presented. Any event involving information at the confidential level or higher must be declared PED 0. Additionally, any sensitive information at the FOUO level, or proprietary information including conditions of contracts, pricing and fees, or pre-decisional support information may be declared PED 0 if disclosure of the information could reasonably be expected to cause harm.

b. PED 1 = Specified PEDs allowed – This category may be used for events not including classified information and at which FOUO, sensitive, or proprietary information may be discussed. Briefers, instructors, or persons in charge of the event will announce the PED designation prior to the event and will provide an area to secure PEDs. Select PEDs include government issued and operated telephones, official photographic equipment, and devices incapable of audio or video recording, such as fitness trackers.

c. PED 2 = All PEDs are allowed – This category applies to all events not specifically restricted under paragraph 5a and 5b above.

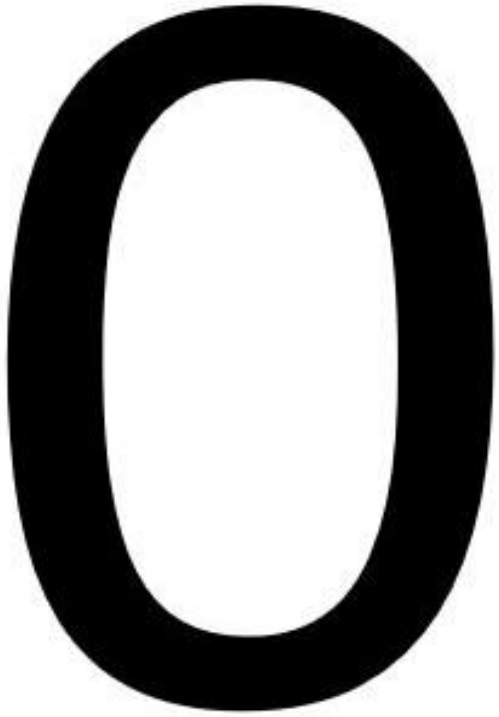
6. The point of contact for this memorandum is the USAG Operations Security Officer, Mr. Rick DeBee at 301-619-1929 or richard.b.debee.civ@mail.mil.

2 Encls
as

SCOTT M. HALTER
Colonel, AV
Commanding

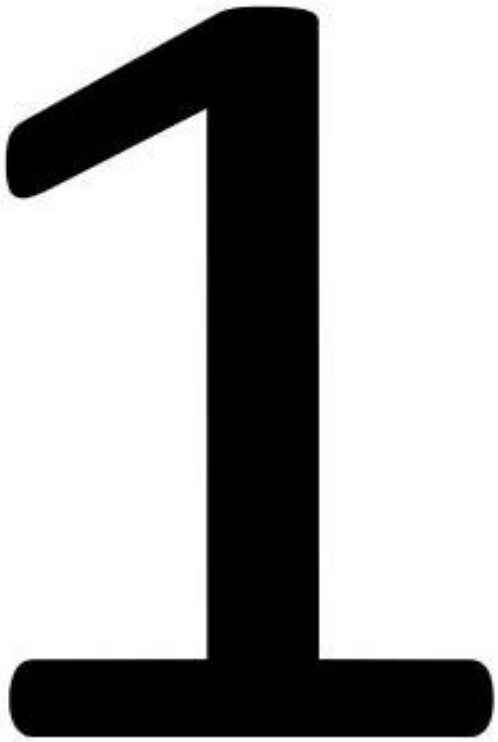
DISTRIBUTION:
B

PED Level



No Personal Electronic Devices Allowed

PED Level



Specified Personal Electronic Devices Allowed

PED Level

All Personal Electronic Devices Allowed

Risks

For sixty years, intelligence services of our adversaries worked to sneak listening devices, transmission devices, and cameras into classified work spaces.

Today…


Smart Phones & Blackberries

- Stores and transmits relatively large amounts of data
- Camera can be used to photograph paper documents or computer screens.
- Can be used as a microphone to record or transmit conversations *without the owner's knowledge*.

Tablets & Personal Computers

- Stores large amounts of data; can also transmit data.
- Camera can be used to photograph paper documents or computer screens.
- Can be hacked for use as a microphone and camera *without the owner's knowledge*.

Smart Watches

- Stores data; can also transmit data.
- Camera can be used to photograph paper documents or computer screens.
- Can be used as a microphone to record or transmit conversations.
- Charging, uploading, and downloading use the same USB cable.

FitBit

- Stores data; transmits via Bluetooth or USB cable.
- Unclassified DAG2 ALARACT says risk is minimal if Bluetooth and USB interfaces are disabled.

Comment: All "smart" devices are capable of staying connected full-time to the internet, via satellite, Wi-Fi, cable, etc. Therefore, these devices provide a means for our adversaries to hack into our network / systems 24/7 without warning.

RED presents a high risk in Collateral areas.
GREEN presents a low risk in Collateral areas.