DEPARTMENT OF DEFENSE
UNITED STATES SOUTHERN COMMAND
9301 NW 33RD STREET
DORAL, FL 33172

REPLY TO
ATTENTION OF

SC-COS

10 October 2013

POLICY MEMORANDUM 07-13

SUBJECT: USSOUTHCOM Wireless Communication and Portable Electronic Devices (PED)

1. References:

a. Memorandum, DoD CIO, 06 April 2011, Subject: Use of Commercial Mobile Devices (CMD) in the Department of Defense.

b. Instruction, CJCS, 24 January 2012, Subject: 6211.02D, Defense Information Systems Network (DISN) Responsibilities.

c. Manual, CJCS, 10 July 2012, Subject: 6510.01B, Cyber Incident Handling Program.

d. Regulation, USSOUTHCOM, SC-COS, TBP (Draft), Subject: Security Incidents.

2. Purpose: To publish guidance for Wireless Communication and Portable Electronic Devices (PED) in areas where controlled unclassified and classified information is processed, stored, or discussed. This includes NIPRNet and SIPRNet systems which are also known as the DoD Information Networks (DoDIN).

This policy supersedes Policy Memorandum 06-11, dated 01 March 2011.

3. Definition.

a. Portable Electronic Devices (PED) is defined as any mobile device, including voice and data systems, with the capability of recording, storing, and/or transmitting information. This includes, but is not limited to cellular phones/smart phones (e.g. iPhone, Droid, Blackberries), Personal Digital Assistants (PDA), two-way pagers, audio/video recording devices, iPods/MP3 players, smart watches, laptops, and tablets (e.g. iPad, Kindle, etc.).

b. Wireless Communication is defined as technology that permits the active transfer of information without physical connection.

4. This policy applies to the following USSOUTHCOM organizations and personnel that utilize or access DoDIN and systems.

a. the Headquarters-Doral Campus, Direct Reporting Units (DRUs), Joint Task Forces (JTFs), Security Cooperation Offices (SCO) and all other organizational entities in operational spaces under the command and control of the USSOUTHCOM Combatant Commander.

b. all military, civilian, contractor, inter-agency, internship, volunteers, foreign and partner nation personnel who are assigned, attached, or visiting USSOUTHCOM facilities.

5. Discussion: Within DoD, for every advantageous use of wireless communications and PEDs there are just as many associated vulnerabilities. Every PED poses a risk for data loss or compromise. If a device is compromised, lost or stolen, sensitive data can potentially fall into the wrong hands. DoD personnel using PEDs must be educated of the appropriate best business practices and operational security countermeasures that can reduce and/or mitigate risk to prevent possible compromises.

6. Policy: Effective immediately, the use of wireless communications or PEDs without the written exception of the USSOUTHCOM J6 Designated Authorizing Official (DAO) is strictly prohibited inside USSOUTHCOM facilities. Facilities/Spaces that utilize USSOUTHCOM provided DoDIN and information systems are subject to the provisions of this policy.

a. Wireless voice communication devices are not authorized within USSOUTHCOM facilities without regard to whether the device may be powered off, set to "airplane mode, silence, or vibrate".

b. Wireless data communication (e.g. text, e-mail, web browsing) is not authorized within USSOUTHCOM facilities.

c. PEDs are prohibited from connecting to information systems (e.g. transferring data, charging batteries, downloading/uploading music, etc.).

7. This policy does not apply to security forces' radios, receive-only pagers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems.

8. All personnel should review the Wireless Communication and Portable Electronic Devices Authorization Chart (encl. 1) to familiarize themselves with the criteria for limited use of some communication devices within USSOUTHCOM work areas and recreational spaces.

9. Connection of limited use devices to any USSOUTHCOM network or information system is strictly prohibited.

10. Requests for exception are determined by the SCJ6 DAO. Further, the Security Cooperation Offices are subject to Embassy Regional Security Official approval. Additionally, if an exception is granted authorizing a wireless communication device and/or a PED, to bring such a device within Sensitive Compartmented Information Facilities (SCIF) further approval would be required from the SCJ2 SSO.

11. Per reference (c) violations of this policy will be considered a Cyber Incident – Category (5) Non-Compliance Activity (Practices Dangerous to Security) and reported as prescribed in reference (d).

12. Violations of this policy may result in punitive or adverse administrative actions or nonjudicial punishment.

13. The points of contact for this policy are Jorge L. Ramos-Soto, SCJ622 Information Assurance Branch, (305)437-3205 or R.E. Jefferson-Miller, (305)437-1631.

FOR THE COMMANDER:

Mark C Nowland

Encl

MARK C. NOWLAND
Major General, U.S. Air Force
Chief of Staff

DISTRIBUTION:
D

Wireless Communication and Portable Electronic Devices Authorization Chart
10 October 2013

Device Type	Permitted for Entry	Approval & Registration Required	Permitted for Use In USSOUTHCOM facilities	Required Mitigation
Government issued PDAs/SME PED/Cellular Phones/Smart Phones**	**No	N/A	No	N/A
Personally Owned PDAs/Cellular Phones/Smart Phones	No	N/A	No	N/A
Personal Laptops	No	N/A	No	N/A
Wireless Keyboard	No	N/A	No	N/A
First Responders & USSOUTHCOM Security Police Government-issued Land Mobile Radio (any gov't issued HF radio)	Yes	N/A	Yes	Not authorized for continuous use within classified space. (Urgent or Emergency use only within classified spaces/Controlled Access Areas).
AM/FM Receive Only Radio	Yes	No	Yes	No
USSOUTHCOM Laptops	**Yes**	Yes	Yes with site J6 Approval memorandum.	**1. Site J6 must record and identify all organizational laptops.** **2. Wireless, Bluetooth, Microphone, and Cameras Lens must be disabled.** **3. DAO approval required prior to connecting to the DoDIN.**
Visitor or Contractor-Owned Laptops	Yes	Yes	Yes with site J6 Approval memorandum.	**1. Formal request must be submitted and approved thru the site J6 prior to entry.** **2. Wireless, Bluetooth, Microphone, and Cameras Lens must be disabled.** **3. Will not connect to the DoDIN.**
USSOUTHCOM Owned Tablet Device and Digital/E- book readers (e.g. Kindle, Nook, iPad)	Yes	Yes	Yes with DAO exception.	**1. Formal request must be submitted and approved thru the DAO prior to entry.** **2. Wireless, Bluetooth, Microphone, and Cameras Lens must be disabled.** **3. Will not connect to the DoDIN.**
Government Issued Cordless Microphones for **Unclassified** Briefings	Yes	No	Yes	**1. Classified information systems in room or operational space must be POWERED OFF.** **2. RF devices are not permitted.**
Government One-Way Pager/Beeper	Yes	No	Yes	N/A
Portable Music Players (e.g. CD Player, iPod Classic, iPod Shuffle, etc.) without Audio/Video recording and Wireless/Bluetooth capabilities	Yes	No	Yes	1. Audio or video recording capability prohibited. 2. Wireless/Bluetooth capability prohibited. **3. Will not connect to the DoDIN or information system.**
Portable Music Players (e.g. iPod Touch, Zune, etc.) Smart Watch, **& any NEW DEVICES** with Wireless, Cameras, Bluetooth, or Microphones capabilities	*Yes	No	**In recreational facilities only (e.g. gym, outside)** **Not in any USSOUTHCOM work spaces**	1. Audio or video recording capability prohibited. 2. Wireless/Bluetooth capability prohibited. **3. Will not connect to the DoDIN or information system.**

***In recreational facilities only (e.g. gym).**
****Government issued communication devices and laptops are authorized for maintenance purposes only.**

NOTE: Mobile device entry into SCIF requires SSO approval

Definitions:

a. Portable Electronic Devices (PED): Any mobile device, including voice and data systems, with the capability of recording, storing, and/or transmitting information. This includes, but is not limited to cellular phones/smart phones (e.g. iPhone, Droid, Blackberries), Personal Digital Assistants (PDA), two-way pagers, audio/video recording devices, iPods/MP3 players, smart watches, laptops, and tablets (e.g. iPad, Kindle, etc.).

b. Wireless Communication: Technology that permits the active transfer of information without physical connection.