UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

5239
SSEC/G6
JUL 25 2016

POLICY LETTER 7-16

From: Commanding General
To: Distribution List

Subj: USAGE OF PORTABLE ELECTRONIC DEVICES WITHIN I MARINE EXPEDITIONARY FORCE (MEF)

Ref: (a) DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid
(b) DoD CIO Memo, Introduction and Use of Wearable Fitness Devices and headphones within DoD Accredited Spaces and Facilities
(c) MCO 5239.2B, Marine Corps Cybersecurity
(d) MCO 3070.2A, The Marine Corps Operations Security (OPSEC) Program
(e) MCO 5100.29B, Marine Corps Safety Program
(f) MARADMIN 274/16, Authorization for Personal Wearable Fitness Devices (PWFD) in Marine Corps Facilities
(g) USMC ECSD 005, Portable electronic Devices, Ver. 2
(h) I MEFO 5101.1, I Marine Expeditionary Force Drivesafe Order

1. Background. The last decade has witnessed a steady rise in the availability, capability, and use of Portable Electronic Devices (PEDs). PED use now, spans a wide range of personal usage, including cameras, watches, communications devices, and fitness monitors to name a few. Subsequently, personal use of these devices is prevalent. PEDs offer great potential but also pose possible vulnerabilities. These vulnerabilities are well documented in the realm of operations security and information assurance; however, PED use also presents a safety risk that must be addressed. Because many PED users have deeply integrated these devices into their personal lives, in forms as diverse as alarm clocks to GPS enabled maps, the risk of distraction in situations that require heightened attentiveness presents a concerning safety risk. It is the responsibility of each individual to continually incorporate OPSEC - identifying critical information and reducing vulnerabilities during the planning, preparation, execution, and post-execution of operations and activities - to contribute to the overall effort for mission success. The individual, categorical vulnerabilities presented through PED use as a singular force protection issue; information protection, operations protection, and individual safety protection must all be viewed through the singular lens of preserving assets vital to I MEF.

POLICY LETTER 7-16

2. Purpose. To promulgate reasonable but enforceable punitive orders that articulate expectations of proper use of PEDs by I MEF personnel. The objective will be protection of assets vital to I MEF, specifically the proper security of our information and safety of our personnel.

3. Information

a. PEDs are defined as any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing or transmitting data, voice, video or photo images. This includes, but is not limited to any form of wireless phones, laptops, cellular "smart" phones, MP3 players, tablets, audio recorders, video cameras and wearable fitness devices.

b. Although the definition of PEDs is broad, the commercial market continues to produce new capabilities that will expand the current definition. Reasonable consideration of new technologies, to include wireless capabilities, should be assumed as a component of this policy.

4. Tasks

a. Commanding Generals, Commanding Officers [I Marine Expeditionary Force Headquarters Group (MHG), 11th Marine Expeditionary Unit (MEU), 13th MEU, 15th MEU)]

(1) Develop and promulgate a directive that provides guidance and, where appropriate, enforceable punitive orders to assigned personnel regarding PED usage. Specific personnel safety expectations will be articulated to include situations or locations where PED use is prohibited due to safety concerns related to distraction. Examples may include but are not limited to; flight line, driver or assistant driver of government vehicles, live fire ranges, etc. Reference (h) provides guidance for tactical, non-tactical, and private motor vehicle operations with reference to use of cell phones.

(2) Provide comments regarding the improper use if PEDs as a form of distraction in mishap reports or investigations that result in the injury of assigned personnel or damage of government equipment.

(3) Develop and promulgate clear enforceable guidance regarding the use of PEDs in government workspaces and settings. Specific attention will be directed to the sharing of pictures, images, and other information that negatively impacts the mission or good order and discipline of the organization. References (a) through (d) provide guidance on information assurance and operations security matters.

b. Inspector General

POLICY LETTER 7-16

(1) Review each commands PED policy during annual Commanding General's Inspections. Assign an appropriate functional area inspection category to ensure compliance.

(2) Capture results of safety reports that identify improper PED usage, specifically as a form of distraction, as a causal factor in mishap reports.

5. Coordinating Instructions

a. Military users in violation of DOD, DON and USMC cybersecurity policies and procedures may be subject to disciplinary actions under the Uniform Code of Military Justice (UCMJ), Federal, and/or State criminal statutes and laws.

b. Violation of this policy by civilian and contract personnel may result in personnel actions under 5 CFR 2635.101(b)(9) and (14), the Federal Acquisition Regulation (FAR), or referral of criminal violations to appropriate civilian authorities.

c. Ensure commands leverage subject matter expertise of OPSEC Program Coordinators to align PED policy with established references and higher guidance.

d. Recommendations for changes to this policy will be submitted to I MEF G6 via the appropriate chain of command.

e. This Policy Letter is effective the date signed.

D. H. BERGER

Distribution: I, II