

RTTUZYUW RUEWMCS0019 0851830-UUUU--RUCRNAV.

ZNR UUUUU

R 251830Z MAR 16

FM SECNAV WASHINGTON DC

TO ALNAV

INFO SECNAV WASHINGTON DC

CNO WASHINGTON DC

CMC WASHINGTON DC

BT

UNCLAS

ALNAV 019/16

MSGID/GENADMIN/SECNAV WASHINGTON DC/-/MAR//

SUBJ/ACCEPTABLE USE OF AUTHORIZED PERSONAL PORTABLE ELECTRONIC DEVICES IN
SPECIFIC DEPARTMENT OF THE NAVY SPACES//

REF/A/DOC/APR 2010//

REF/B/DOC/FEB 2012//

REF/C/DOC/OCT 2015//

REF/D/DOC/FEB 1996//

REF/E/DOC/APR 2004//

REF/F/DOC/NOV 2009//

REF/G/DOC/JUN 2006//

REF/H/DOC/JUN 2006//

REF/I/MSG/JAN 2016//

NARR/REF A is Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary". REF B is DoDM 5200.01-Volume 3, Department of Defense (DoD) Information Security Program: Protection of Classified Information. REF C is Deputy Director of Naval Intelligence (N2N6I): Department of the Navy Sensitive Compartmented Information Facility Personal Portable Electronic Devices Clarification Memorandum, dated 26 October 2015. REF D is Federal Communications Commission Office of Engineering and Technology Bulletin Number 62, Understanding the FCC Regulations for Computers and Other Digital Devices. REF E is DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). REF F is DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies. REF G is SECNAV M-5510.36, Department of the Navy Information Security Program Manual. REF H is SECNAV M-5510.30, Department of the Navy Personnel Security Program Manual. REF I is ALNAV 001/16, Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on Department of the Navy Information Systems//

POC/Mr. Mark Myers/CIV/DUSN(P) Security/TEL: (703)601-1019/DSN: 225-1019/EMAIL: mark.a.myers2@navy.mil/ Mr. James Mauck/CIV/DON CIO Cybersecurity and Infrastructure Team/TEL: 703-695-1893/EMAIL: James.Mauck@navy.mil//

RMKS/1. This is a coordinated Deputy Under Secretary of the Navy Policy (DUSN(P)) Security, and Department of the Navy Chief Information Officer (DON CIO) message as part of the Department of the Navy's (DON) cyber/traditional security partnership for the protection of national security information and information systems.

2. Purpose and Definitions. The purpose of this ALNAV is to provide interim policy for acceptable use of personal portable electronic devices (PPEDs) in specific DON spaces based on device capability. Terms used in this ALNAV are defined below:

a. A portable electronic device (PED) is defined in REF A as any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images (e.g., cell phones, laptops, tablets, and wearable devices such as fitness bands and smart watches).

b. "Personal" in this message refers to PEDs personally owned by DON Sailors, Marines, civilians, and support contract personnel.

c. Commanding Officer (CO) in this message is a generic term used to identify a position of authority at any DON organization, base, station, unit, laboratory, installation, facility, center, activity, detachment, squadron, ship, battalion, regiment, etc.

d. Homeland connotes the continental United States, Alaska, Hawaii, United States possessions and territories, and surrounding territorial waters and airspace, per REF B.

e. Near Field Communication (NFC) connotes a short-range wireless communication system employing radio waves to enable a mobile device to interact with another device or card reader when within 10 cm (4 in) of each other.

3. Scope and Applicability. This ALNAV applies to all DON Sailors, Marines, civilians, and contract personnel regarding the use of PPEDs with specific capabilities in spaces where collateral classified information is processed, transmitted, stored, or discussed. Non-DON personnel are prohibited from introducing PPEDs into DON spaces. This ALNAV does not prevent COs from issuing stricter policy in accordance with the needs of their commands; authorize introduction of PPEDs into any DON spaces located outside the homeland or in Sensitive Compartmented Information Facilities (SCIFs) (see REF C); or apply to PEDs issued by the DON for official business.

4. Discussion. The proliferation of PPEDs in the form of wearable technology has increased dramatically since the introduction of wearable heart rate monitors in the 1980s. Today's portable electronic activity monitoring devices, (e.g., fitness, communication, and medical) offer a wide range of personal, professional, and health benefits. However, these devices may pose security risks to DON information and information systems. This message specifically identifies capabilities associated with PPEDs that are permitted in DON spaces where collateral classified information is processed, transmitted, stored, or discussed in order to allow PPED use while minimizing risk to DON information. It also lays the groundwork for future DON wireless policies.

5. Action. Effective immediately, all DON personnel using PPEDs in DON spaces where collateral classified information is processed, transmitted, stored, or discussed must comply with the requirements and responsibilities cited below:

a. PPEDs are permitted:

(1) If commercially obtained in the U.S. or through a U.S. military exchange and assigned a Federal Communication Commission (FCC) Identifier denoting compliance with the limits for a Class B digital device designated by the FCC, pursuant to Part 15 of the FCC Rules, per REF D.

(2) If they contain only vendor-supplied software and receive only updates that do not add any features or capabilities prohibited in this message.

(3) If they have any or all of the following: Bluetooth, Global Positioning System (GPS) (RECEIVE-ONLY), accelerometer, altimeter, gyroscope, heart monitor, vibration, and/or NFC capabilities.

(4) If they have password/pin protections enabled and have up-to-date anti-virus software protection installed, where those capabilities exist.

b. PPEDs are prohibited:

(1) If they contain cellular and/or Wi-Fi transceivers, or other technologies not permitted in para 5.a. of this ALNAV.

(2) If they have photographic, video capture/recording, microphone, and/or audio recording capabilities.

(3) From being connected to any government information system either directly or indirectly using wired or wireless accessories (e.g., Bluetooth dongles and charging cables).

(4) If they have removable media installed.

(5) If they have the capability to perform radio frequency transmissions at greater than 100 milliwatts (mW) Equivalent Isotropically Radiated Power (EIRP). Where feasible, EIRP shall be determined using FCC data.

c. Commanding Officers:

(1) Ensure dissemination and enforcement of this policy, employing either technical monitoring per REFs E and F or through physical checks, spot checks, and/or physical searches.

(2) Ensure compliance with the security incident reporting requirements of REFs B, G, H and I. DON personnel who knowingly and willfully violate the requirements in this message are subject to preliminary inquiry and incident reporting in the Joint Personnel Adjudication System, potential loss of information system access, and possible punitive or administrative action.

(3) May grant interim approval for medically related PPEDs when the capabilities they possess are prohibited by this message. In those instances, the Navy or USMC Authorizing Official must be notified within 30 days of device make/model, the capability presenting risk, and the proposed mitigation.

d. DON personnel:

(1) Ensure PPEDs meet the criteria in para 5.a, prior to introducing them into areas where collateral classified information is processed, transmitted, stored, or discussed.

(2) Ensure the CO has not levied additional restrictions or

prohibitions prior to introducing PPEDS in DON spaces where collateral classified information is processed, transmitted, stored, or discussed.

(3) Obtain approval, per para 5.c(3) of this ALNAV, for any medically related PPEDs prior to introduction into areas where collateral classified information is processed, transmitted, stored, or discussed.

6. This ALNAV remains in effect until incorporated in future DON wireless policy and REF G for safeguarding and reporting requirements.

7. Released by Ray Mabus, Secretary of the Navy.//

BT

NNNN

UNCLASSIFIED//