DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVENUE
WASHINGTON NAVY YARD DC 20376-2101

IN REPLY REFER TO
Canc frp: May 2017

NAVSEANOTE 2200
Ser 00I-019/144
19 May 2016

NAVSEA NOTICE 2200

From: Commander, Naval Sea Systems Command

Subj: UPDATE TO NAVAL SEA SYSTEMS COMMAND PHOTOGRAPHIC, AUDIBLE RECORDING AND PORTABLE ELECTRONIC DEVICES POLICY

Ref: (a) NAVSEAINST 2200.1
(b) NAVADMIN 216/15
(c) SECNAV M-5510.36
(d) OPNAVINST N9210.3
(e) ALNAV 019/16 of Mar 2016

1. Purpose. This notice updates and clarifies reference (a) in regard to Personal Wearable Fitness Devices (PWFD), Tablets and Portable Electronic Devices (PED).

2. Background. Reference (a) is the current Naval Sea Systems Command (NAVSEA) PED Policy. Reference (b) provides a definition of and guidance on PWFD. This notice updates reference (a) and supersedes identified items while changes are incorporated into the next revision.

3. Scope and Applicability. A PED is defined in reference (c) as an easily transportable electronic device which has a capability to record, copy, and store and/or transmit data, digital images, video and/or audio. This notice applies to all devices broadly meeting the PED definition above and includes Government-owned, personally-owned, and contractor-owned devices. The portion of the notice providing PWFD authorization is applicable to spaces located within the Continental United States, Alaska, and Hawaii; PWFDs are not currently authorized for use in NAVSEA facilities outside of these identified areas.

4. Exclusions. This authorization does not address wearing PWFDs in Sensitive Compartmented Information Facilities or areas authorized for Special Access Programs (SAP). This notice does not apply to equipment specifically exempted by higher guidance, i.e. Communications Security equipment or material. This notice

is not applicable to properly credentialed law enforcement or Inspector General personnel in performance of their official duties. This notice does not authorize introduction of any device into spaces performing industrial manufacturing or industrial control processes in connection with Naval Nuclear Propulsion Information (NNPI) without consent of SEA 08.

5. Action. All military, Government civilian, and contractor personnel assigned to NAVSEA Head Quarters (HQ) Staff Codes, affiliated Program Executive Office's shall comply with this policy. NAVSEA Field Activities shall minimally comply with this policy; however, more restrictive policies may be locally directed to meet mission requirements and capabilities. The authorizations for entry of devices as outlined in this notice do not apply to contractors not "seated", i.e. assigned a workspace within NAVSEA facilities.

6. Policy. This notice prohibits use of any PED within an area authorized for processing classified information, or within an area where any classified discussion is taking place, and prohibits connection of any device to a Government-owned computer except as otherwise authorized. Reference (e) provides the acceptable uses of authorized personal PED within specific Department of the Navy spaces. This notice authorizes entry of devices defined above as follows:

a. Government-owned devices are generally authorized into NAVSEA facilities and spaces except as outlined in paragraph 6.d below.

(1) Government-owned devices are required to comply with applicable instructions.

(2) Government-owned devices such as iPhones are currently prohibited from connecting to NMCI computers.

(3) Government-owned devices are NOT authorized by this notice to enter or operate in spaces processing classified information.

(4) Government-owned devices are authorized within basic office spaces, including those processing Unclassified NNPI. In such spaces, sound judgment is required prior to conducting discussions. Although PEDs are authorized in these locations,

each employee is responsible to ensure that controlled information is not inadvertently exposed to unauthorized personnel and recording of any kind is prohibited.

(5) Where Unclassified NNPI, as defined by reference (d) or applicable security classification guides, is exposed or discussed in unclassified or open access spaces, the following requirements apply:

(a) Government, shipyard employees, and military members who possess Government issued cell phones, and do not have an authorized Shipyard or Naval Reactors band, must have their device verified by the shipyards IT personnel to ensure that the camera and recording devices have been disengaged as a part of a Government approved configuration prior to entry into the controlled industrial area (CIA). Upon verification by shipyard IT personnel, a shipyard band will be placed on the Government issued phone and they should be authorized to take their phone onto the shipyard to include the CIA. The shipyard band and Naval reactors bands should be honored by all shipyards. This guidance does not take away the commanding officer's authority to implement prudent and appropriate security precautions, nor their ultimate responsibility for the protection of sensitive information within their Command.

b. Personally-owned and "seated" contractor-owned devices are authorized in NAVSEA facilities and spaces as follows:

(1) Cellular telephones and "smartphones" are authorized in NAVSEA facilities and spaces.

(2) Lightweight electronic tablets (under two pounds) without a permanently attached keyboard (such as the Apple "iPad" and Microsoft "Surface") are authorized in NAVSEA facilities. While these devices are authorized in the facility, these devices are NOT authorized to process or contain any information that has not been authorized for public release. *Note: Processing Controlled Defense Information on contractor-owned information systems has specific requirements which are not covered by this notice.*

(3) Laptop computers are not authorized under this notice.

(4) Wi-Fi Hotspot services provided by devices authorized under this section are required to be disabled while in NAVSEA facilities.

(5) Devices under this section are NOT authorized to enter or operate in spaces processing classified information.

(6) Devices under this section shall be excluded from any location where physical manifestations of NNPI exist, such as components, collections of components, or systems or where component and/or system manufacturing and assembly occur. Examples include, but are not limited to, fabrication and assembly areas, component lay-down and storage areas, machine shops, and warehouses containing NNPI or processes and/or tooling critical to NNPI work. Appropriately configured Government and contractor issued PEDs shall continue to be governed by local and higher-tier guidance as appropriate.

c. Wi-Fi Hotspots:

(1) Government-owned Wi-Fi Hotspots will not be placed in service within NAVSEA facilities without written authorization of the cognizant Command Security Manager (CSM) and Information Systems Security Manager (ISSM). Within NAVSEA HQ, SEA 00P and the HQ IAM (SEA 00I) are the cognizant authority.

(2) Government-owned Wi-Fi Hotspots are not authorized in areas processing Sensitive Compartmented Information (SCI) or areas authorized for SAP without prior authorization of the cognizant Special Security Officer (SSO).

(3) Government-owned Wi-Fi Hotspots will not be authorized without a clear operational requirement that cannot be otherwise satisfied.

(4) Government-owned Wi-Fi Hotspots will be configured per the current applicable Defense Information Systems Agency Security Technical Implementation Guide(s) prior to being placed in service.

(5) Authorization of any Wi-Fi Hotspot by a field activity will be forwarded to the NAVSEA Command Information

Office (SEA 00I) Cybersecurity Resource Desk (NAVSEA_CSRD@navy.mil) and are subject to review by the NAVSEA Command Information Officer.

(6) Non-Government owned Wi-Fi Hotspots are not authorized. Hotspot services provided by authorized devices such as cellular telephones are required to be disabled while in NAVSEA facilities.

d. Personal Wearable Fitness Devices:

(1) NAVSEA assigned personnel are hereby authorized, subject to local policy and capability limitations, to wear PWFDs (e.g., Fitbit, Jawbone Up, Nike Fuel Band, etc.) in all NAVSEA spaces where collateral classified and/or controlled unclassified information is processed, stored, or discussed as long as the device has no Wi-Fi, cellular, or audio/video recording capability.

(2) NAVSEA assigned personnel (civilian, military, and seated contractors) wearing PWFDs must: read and comply with reference (b); acknowledge in writing or signed email to their supervisor that they have read reference (b) and that the device meets the referenced requirements. This acknowledgement must be maintained by the employee's supervisor as long as the device is worn within NAVSEA facilities.

(3) Employees who are unsure if their PWFD is in compliance with the standards shall notify their supervisor who shall obtain guidance and approval through the NAVSEA Cybersecurity Resource Desk at NAVSEA_CSRD@navy.mil prior to introducing it into NAVSEA facilities.

7. Violations. Any violation of this instruction involving an area where classified information is processed or discussed is required to be reported to the CSM and ISSM for a potential adverse action report and disciplinary action. Additionally, any violation in an area involved with SCI is also required to be reported to the SSO.

8. Records Management. Records created as a result of this notice, regardless of media or format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

9. Cancellation Contingency. This notice is in effect for 1 year or until it is superseded by another notice or an update to the instruction, whichever occurs first.

W. H. HILARIDES

Distribution: Electronic only, via the NAVSEA Intranet Web site located at https://navsea.portal.navy.mil