



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 2060.1
BUPERS-07
19 Sep 2017

BUPERS INSTRUCTION 2060.1

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL POLICY FOR USING NAVY MOBILE DEVICES (SMART PHONE/TABLETS)

Ref: (a) CNO WASHINGTON DC 211645Z Apr 15 (NAVADMIN 092/15)
(b) DON CIO memo, Subj: DON Mobile (Cellular) Services Cost Management of 1 Aug 2014
(c) DON CIO WASHINGTON DC 281759Z Aug 12

Encl: (1) DON Policy For Achieving Mobile (Cellular) Services Cost Efficiency

1. Purpose. This instruction provides information and guidance for the use of government-issued mobility devices in support of the advancement of information technology (IT) wireless services on the Navy Marine-Corps Intranet (NMCI).
2. Scope and Applicability. This instruction applies to all military and civilians who request mobile devices from Bureau of Naval Personnel (BUPERS), NMCI Support Branch (BUPERS-0711).
3. Policy. The U.S. Navy enables workforce mobility using commercial mobile devices and services. To ensure these capabilities are delivered and employed cost-effectively, all BUPERS commands must actively review and manage associated investments per references (a) through (c). Reference (a) promulgated stipulations for using Navy mobile devices (smart phones and tablets). Reference (b) provides policy for managing mobile services to minimize the cost of workforce mobility capabilities. Reference (c) updated policy for disposal of electronic media storage.
 - a. Mobility is transforming how the Navy operates, connects, and supports our personnel and the fleet. To meet this growing demand the Naval Enterprise Networks (NEN) Program Office (PMW-205) has implemented a mobile solution to meet operational needs while complying with architectural and security requirements to protect the Navy enterprise. Android and newer iPhone/iOS versions will be supported as they are released and certified for operation on the NMCI network. Information, processes, and user guides and acknowledgement are available at <https://www.homeport.navy.mil/services/mobile>.
 - b. New devices will use a Good Technology (trademark) container to securely segregate official data from personal data, thereby providing users the ability to perform government work and personal activities securely and effectively on the same device per U.S. Navy policies on

acceptable use of government IT. Mobile device configuration, security settings, and policy enforcement will be managed using Good Technology (trademark) mobile device management software and equipment installed on NMCI.

c. The improved service will be available to users who are approved by their local command and can be ordered as a standard wireless device update through the command's wireless account manager, BUPERS, Capital Planning/NMCI Division (BUPERS-071).

d. Per reference (a), the following stipulations apply:

(1) Use of personally owned devices is not authorized.

(2) Access to the Good Container will be controlled via a minimum eight character passcode containing alpha-numeric and special characters.

(3) Commands and users are responsible for adhering to all applicable physical security requirements for portable electronic devices in command spaces.

(4) The camera will be turned on by default, with the option to have it turned off per individual or as directed at the command level. Cameras on government furnished equipment devices will be subject to wireless security restrictions imposed by the facility in which the device is being operated. Cellular and personal communications service (PCS) and or other radio frequency or infrared wireless devices must not be allowed into an area where classified information is discussed or processed without written approval from the Navy authorizing official in consultation with the Cognizant Security Authority Certified Transient Electromagnetic Pulse Emanation Standard Technical Authority.

(5) Non-work applications may be installed only outside the Good Container and may only be acquired from the iTunes/Google app stores. Users are responsible for all charges and installations of personally desired applications and data installed on the non-secure portion of the device.

e. Department of Defense (DoD) Instruction 8520.02 of 24 May 2011 requires all DoD information systems, including networks and email, be enabled to use DoD-issued public key infrastructure certificates in order to support authentication, access control, confidentiality, data integrity, and non-repudiation. Department of the Navy (DON) users must digitally sign all email messages with attachments, active content, or which require either message integrity or non-repudiation verification. Email messages containing sensitive information must be encrypted. Transmission of email (i.e., create, forward, reply, and reply all) that should be either signed or encrypted without applying digital signature or encryption is prohibited, regardless of technical limitations of the desktop or handheld device being used.

f. Per reference (b), as responsible stewards of public funds, all BUPERS activities must actively manage their mobile services to minimize the cost of necessary capabilities. As such,

19 Sep 2017

BUPERS employees and commands are directed to adhere to the DON policy for achieving mobile (cellular) services cost efficiency practices in enclosure (1).

4. Point of Contact. BUPERS, Command Information Office (BUPERS-07) is the point of contact.

5. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV M-5210.1.

6. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-07 will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, Department of Defense, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. OPNAV 5215/40 may be obtained from the BUPERS directives manager. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.



R. A. BROWN
Deputy Chief of Naval Personnel

Releaseability and distribution:

This instruction is cleared for public release and is available electronically only via BUPERS Web Site, <http://www.public.navy.mil/bupers-npc/Pages/default.aspx>

DON POLICY FOR ACHIEVING MOBILE (CELLULAR)
SERVICES COST EFFICIENCY

1. Zero-Use Devices

a. Zero Minutes. If a cellular device reflects zero minutes of use on three consecutive monthly invoices, the responsible activity will re-validate the need for that device or cancel the service.

b. Continuity of Operations (COOP). Cellular devices intended solely for COOP purposes will be on rate plans that minimize the monthly cost of maintaining inactive devices. Though carrier-dependent, the best option for these devices is usually the lowest cost-metered ("pay as you go") service plan.

c. Monitoring. The Department of the Navy (DON) Chief Information Officer (CIO) monitors zero use devices. Each quarter, in cases where activities have not initiated appropriate action to minimize costs, the DON CIO will direct those activities to modify their task orders. Progress will be monitored through Fleet Logistics Center, San Diego.

2. Pooled-Minute Usage Management

a. Over-Utilization. An activity with a pooled-minute plan or a device with an assigned minute plan that is charged for exceeding its limits by 25 percent or more for three consecutive months is required to change to a plan or pool with more minutes.

b. Under-utilization. An activity with a pooled-minute plan or a device with an assigned minute plan that is charged for 75 percent or less of the contracted minutes for three consecutive invoices is required to change to another plan with fewer minutes.

3. Air Cards. DON personnel assigned data-capable devices (e. g., smartphone or BlackBerry) will not be issued air cards to provide Internet connectivity for their laptop computers. Instead, those personnel will employ a "tethering" option; using the phone as a modem to provide unlimited data connectivity at no additional cost.

4. Expense Management Tools and Training

a. Online Tools. All DON activities will employ the no-cost online tools and data made available by the service providers (Verizon, AT&T, etc.) to manage their accounts for maximum efficiency.

b. Training. All DON account managers who will have the authority to order, cancel, or modify services via the DON wireless contract must be trained to use the wireless management tool by the appropriate carrier within 90 days of assignment. All account managers already exercising such authority must complete the training within 120 days of the date of this

instruction. The training is provided under the wireless contract, either in Fleet Logistics Center San Diego-sponsored classrooms or using on demand WebEx and telecommunications from the carriers.

5. Outside the Continental United States Travel. Use of international calling and data plans for devices to be used on foreign travel must be pre-approved by the contract technical representative. The number of international lines and funding is limited and use will be closely monitored. If use while on travel is excessive, the capability may be terminated. Any traveler must request international capability via their information systems coordinator at least 1 week prior to travel.

6. Task Order Consolidation

a. Navy echelon 2 budget submitting offices (BSO) and Marine Corps major subordinate commands (MSCs) will aggregate mobile device requirements throughout their organizations and make consolidated orders. Some echelon 2 commands have already succeeded in lowering costs by awarding one order with each service provider for each funding type (e.g., operations & maintenance and Navy working capital fund) used to acquire mobile services.

b. If unable to comply with stated guidance to consolidate wireless task orders at the MSC/BSO level, commands and activities must submit waiver and exemption requests to the DON CIO. Requests will consist of formal letter endorsed by the first general officer or senior executive service in the requesting command or activity chain and routed through their respective DON deputy CIO to the DON CIO.

7. Equipment Exchange

a. Recycling old wireless devices and accessories through third parties is not authorized. Account managers are only authorized to exchange wireless equipment from wireless carriers as permitted by the DON wireless contract in compliance with DoN policy (available in the Policy & Guidance section at www.doncio.navy.mil). Wireless equipment exchange only permits the acquisition of like equipment or the exchange of non-surplus or obsolete equipment and will not be used for services or be conducted with vendors not authorized by the DON wireless contract.

b. The DON CIO is working with the Navy and Marine Corps staffs to establish blanket waivers of DON requirements in reference (c) to maximize the DON's wireless equipment buyback potential.