DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

CNICINST 2000.2B
N00
21 Mar 16

CNIC INSTRUCTION 2000.2B

From: Commander, Navy Installations Command

Subj: POLICY AND PROCEDURES ON THE USE OF GOVERNMENT-OWNED WIRELESS DEVICES

Ref: (a) DoDD 8100.02 of 14 Apr 04
(b) OPNAVINST 2100.2A
(c) SECNAVINST 7320.10A
(d) DoD CIO Memo, Optimizing Use of Employee IT Devices and Other IT to Achieve
(e) CNO WASHINGTON DC 211645Z Apr 15 (NAVADMIN 092/15)
(f) CNO WASHINGTON DC 041431Z May 12 (NAVADMIN 152/12)
(g) DON CIO Memo, Department of Navy (DON) Mobile (Cellular) Services Cost Management, of 1 Aug 14
(h) DON CIO Memo, Department of the Navy iOS/Android Capability Deployment, of 24 Feb 15
(i) DON CIO Memo, Department of the Navy Approval of Good Mobility Mobile Computing (UGMMC) V2, of 21 Apr 15
(j) CNICINST 12600.1B
(k) OPNAVINST 2060.8A

1. Purpose. To issue policy and procedures governing the management and use of government owned wireless devices by Commander, Navy Installations Command (CNIC) personnel in accordance with references (a) through (k).

2. Cancellation. CNIC Instruction 2000.2A dated 2 November 2012.

3. Background. The use of Federal government communication systems and equipment is governed by reference (a), which requires that these systems be utilized for official use and authorized purposes only, and that commands manage and administer their use properly. In accordance with reference (b), the Department of Navy Chief Information Officer (DON CIO) requires that a high priority be placed on actions to improve accountability and management of government issued wireless

devices. CNIC is issuing this policy to meet these objectives, ensure we are implementing best practices, and provide the most economical solution to meet command requirements.

4. Policy. These updated policies and procedures apply to CNIC Headquarters (HQ), Regions, and Installations. CNIC Information Officer (N6) will establish oversight and audit actions to enforce the proper use of government-owned wireless devices in accordance with references (c) through (i).

a. Official Use. Government-issued wireless devices will be used for conducting official government business. Wireless device users may also use the device for personal purposes providing that individual use does not create additional expense to the government. Authorized personal purposes shall include a reasonable number of calls made by employees, while traveling on official business, to notify family of official transportation, scheduling, and/or emergency situational changes.

b. Authorization for wireless devices are defined for the following personnel categories:

(1) Command and Staff Personnel. Defined as management personnel involved with the exercise of command and control of CNIC employees executing the CNIC mission.

(2) Essential Emergency Personnel. Defined as command designated personnel providing necessary support critical to the safe operation of the CNIC activities and mission execution 24/7 (to include all emergency type personnel). The requesting supervisor must verify employee has a DD Form 2365 (Department of Defense (DoD) Civilian Employee Overseas Emergency Essential Position Agreement) on file in order to issue a device under this category. Overseas CNIC Region commands must comply with local procedures when employing the essential emergency personnel process.

(3) Key Personnel. Defined as personnel who have responsibilities in the chain of command and require immediate notification of critical issues and/or direct access by higher authorities.

(4) Special Requirement Personnel. Defined as personnel who perform frequent travel or unique duties which require a dedicated cellular telephone or wireless device; this will be

validated and approved at the Region/Installation level. CNIC HQ N6 will validate/approve HQ special requirements. This category includes issuing wireless devices on a temporary loaner basis to support short duration travel or short term mission and/or operational needs.

(5) Issuing government owned mobile devices to dependents of military and civilian personnel is not authorized. A waiver may be granted if the designated individual is employed or directly supports the CNIC Ombudsman Program.

(6) Wireless devices are not authorized for teleworking, unless personnel also fall into one of the other personnel categories listed in section 4.b. (1) thru 4.b. (4) above and have a validated need as part of their position. In accordance with reference (j), no personnel shall be granted a wireless device when the only requirement is teleworking. Office phones shall, instead, be transferred to the personal device of the personnel teleworking to ensure both transparency and that employees are in fact at their alternate worksite.

c. Usage Restrictions. Users issued government wireless devices must adhere to the following guidelines:

(1) When Contiguous United States (CONUS) users are required to perform official international travel, their service plan may be temporarily expanded to include international voice and data service (where available). It should be noted that air card and cellular phone devices do not offer international data pooling so the traveler may be issued a loaner smartphone to support official travel if the Region/installation has an available device. Users must request international service by submitting a justification letter through their N-code Director and then submitted to the Region N6 for approval. International voice and data service are not authorized while on personal leave unless a unique mission requirement dictates such use. The justification letter must indicate location and travel dates to ensure international voice and data service is available for the travel area.

(2) The government employee assigned the cellular phone or mobile smartphone is responsible for safeguarding its usage and must surrender the device to a designated official, either the Region N6 or Installation N6, upon termination, transfer, or internal reassignment.

(3) Stolen or missing wireless devices must be reported immediately to the Region N6 or designated Information Technology (IT) representative so service can be cancelled and preclude illegal use and/or unauthorized charges. This event should be reported and documented by the local Wireless Device (WD) manager by filling out a DD Form 200 (Financial Liability Investigation of Property Loss) report. Authorized cellular telephone and wireless device users may be responsible for reimbursing the government for the purchase price of a lost or stolen cellular telephone or wireless device if loss or theft is determined to be the user's fault or due to negligence.

(4) Authorized cellular telephone and wireless device users are responsible for reimbursing the government for all unauthorized charges (including by other individuals). The process of reimbursement can be documented and reviewed by auditing and monitoring local monthly billing statements.

(5) Wireless device users are not permitted to text message to any international telephone or cellular number or text message back to the United States while overseas, unless specifically authorized by the CNIC/Region N6. Although unlimited free domestic text messaging is authorized, personnel who text message to any international telephone number and text message back to the United States while overseas may be liable to reimburse the government for any charges accrued for excess data charges.

(6) Typically, authorized wireless device users are issued one device only. If special circumstances require that a user be issued multiple wireless devices (Smartphone, Aircard, iPad/Tablet etc.), the user must provide written justification validated by his/her N-Code and Region N6 to the CNIC HQ N6 for approval.

5. Responsibilities

a. CNIC HQ N6 is responsible for:

(1) Developing CNIC wireless policy, managing enterprise wireless devices, acting as the Contracting Officer Representative (COR) for the various wireless commercial contracts, and coordinating within DON CIO for changes to wireless policy guidance.

(2) Coordinating smartphone and cellular phone services with contract providers, managing and placing orders consistent with policy and budget, and communicating program guidance to end users and Region N6's. Coordinate with Region N6's and WD Managers in the management of their local cellular phone programs, troubleshooting and resolving problems, and supporting special requirements.

b. CNIC HQ Enterprise and WD Manager shall:

(1) Support the contracting officer and his/her representative in the solicitation, awarding, and administration of the cellular phone contracts for CNIC users.

(2) Manage and coordinate equipment and service orders with the various contracted providers.

(3) Ensure adherence to current and future cellular phone and wireless devices policy and directives issued by higher echelons, and communicate this policy throughout the CNIC enterprise.

(4) Monitor usage and manage compliance across the CNIC enterprise.

(5) Review, at least monthly, international calling and data plans for devices to be used on foreign travel, in order to minimize high Outside the Contiguous United States (OCONUS) usage charges.

(6) Manage and populate the CNIC N65 Managed IT Services supported Wireless Management on the CNIC Gateway 2.0 (G2) site with the latest billing reports and governing instructions.

(7) Be proficient in the use of the wireless management tool by the appropriate carrier within 90 days of assignment. The training is provided under the wireless contract, either in Fleet Logistics Center San Diego sponsored classrooms, or via on demand WebEx and teleconferencing from the various carriers.

c. Region N6s are responsible for appointing a primary and secondary WD Manager for proper oversight and management. Responsibilities include performing troubleshooting and maintenance activities, updating and replacing equipment,

migrating users between providers as necessary, oversight and reconciliation of Region account billing, usage, and device inventory.

d. Region Cellular Phone and WD Manager shall establish control and proper use of government-owned cellular telephones and wireless devices. The following oversight and audit actions are directed:

(1) Manage equipment and service orders with contracted providers via the CNIC Enterprise WD Manager.

(2) Ensure adherence to current and future wireless policy, guidance, notes and directives issued by higher echelon authorities, and communicate this policy throughout the Region.

(3) Monitor usage and manage compliance across Region.

(4) Perform monthly validation and reconciliation of all wireless devices to ensure up-to-date management data and inventory accuracy.

(5) Submit summary monthly reports on the G2 to the CNIC Enterprise WD Manager. Reports should be submitted by both CONUS and OCONUS Regions regardless of contract origination no later than (NLT) the 10th of each month, and upload to the specific Region reports and billing section.

(6) Forward wireless device user actions to relevant supervisors and/or notify the CNIC Enterprise WD Manager to take action to suspend, restrict or cancel lines when there is a determination of abuse by a user.

(7) Review minute usage to determine if the most economical plan has been obtained for the government and make recommendations to the CNIC Enterprise WD Manager.

(8) Review and report Region and vendor record reconciliations to the CNIC Enterprise WD Manager on a quarterly basis. Reports should be submitted by both CONUS and OCONUS Regions regardless of contract origination NLT the 15th of each quarter (15 January, April, July, and October) for the preceding quarter, and upload to the designated Region reports and billing section.

(9) Ensure all new wireless device requestors have completed Information Assurance (IA) Cyber Security Awareness Challenge training and provided a copy of their completion certificate to the Telecommunications Control Officials (TCO) or Region WD Manager.

(10) Ensure all wireless device users sign and submit a Wireless Device User Agreement and Privacy Acknowledgement to the Region WD Manager. Refer to paragraph 8.0 for the G2 link to forms and reports.

(11) Upon receipt of a monthly vendor report, review the monthly report, verify the accuracy of the report, identify and report any calls that were deemed out of the ordinary or with excess data and voice minutes needing review to the CNIC HQ WD Manager, Region TCO, or WD Manager. Repeat violators will be referred to the Region Commander and Installation Commanding Officer respectively for disciplinary actions resulting in device deactivation until documented counseling has been provided to reactivate the user device.

(12) Validate the need for the device, cancel or modify the wireless line of service for any user that accrues three consecutive months of zero usage in accordance with reference (g). The Region WD Manager will notify the CNIC WD Manager of lines to be modified, cancelled, or reassigned, if devices are considered essential. The device can also be placed in one of the Continuity of Operations (COOP), Emergency Management, or Special Program device pools.

(13) Ensure cellular devices intended solely for COOP purposes will be on rate plans that minimize the monthly cost of maintaining inactive devices.

(14) Employ the no-cost online tools and data made available by the service providers to manage their accounts for maximum efficiency.

(15) When supporting requirements to replace a device due to malfunction, the WD HQ, Region, or Installation manager will provide the specific issue, describing the problem related to the malfunction in formal correspondence for review. The local WD manager and/or COR will coordinate with the vendor to determine warranty and eligibility for device replacement. No

replacement will be approved until the issue is resolved contractually.

(16) Ensure all cellular phones and mobile devices under contract meet eligibility and refresh requirements for replacement based on contract issued date. The CNIC's WD manager and/or COR and shall coordinate with the specified wireless vendor to review device history and determine refresh eligibility status.

(17) When requesting detailed call logs for cellular and mobile devices in support of the Office of General Counsel (OGC), Inspector General (IG), Legal, and Merit System process proceedings, formal correspondence must be provided by the requestor. The formal correspondence, at a minimum, must provide the mobile or phone number, dates for reference, and equipment serial number information. WD managers will complete a non-disclosure agreement (NDA) form for civilians and contractors and provide a copy to the legal counsel office. The WD manager and COR will coordinate detail log requirement processing. It's important to note that this process may be lengthy and take several weeks to retrieve logs, as response times vary among the wireless contract vendors.

6. Enterprise Wireless Device (WD) Management (Smartphone - IOS/Android)

a. Like the rest of the Navy, mobility is transforming how CNIC operates, connects, supports, and enables our personnel to execute the CNIC mission and support to the Fleet, Fighter, and Family. "Smartphones" and "Tablets" are tools becoming available as of fiscal year (FY) 16 and beyond. Initially, CNIC is in the process of deploying iPhone 5s/6 and iPads running iOS 8 to those existing Blackberry (BB) users, in the window for technical refresh, and is part of the Navy's transition off of BB devices to be completed sometime in FY16.

(1) New Smartphones and Tablets will use the "Good" Technology container in order to securely segregate official data from the user's personal data, thereby providing CNIC employees the ability to perform government work while allowing personal activities separately. This is a significant change from the way CNIC has done business in the past, when government and personal hardware were physically separated. Going forward, mobile device configuration, security settings, and policy

enforcement will be managed using "Good" Technology mobile device management software and equipment installed by Navy's Next Generation Network (NGEN), in accordance with references (e) and (j).

(2) Non-work applications may be installed only outside the Good Container and can be obtained from the iTunes/Google application stores only. Users are responsible for any charges and installations of personally desired applications and data installed on the non-secure portion of the device. When a user's smartphone device is activated, an iTunes account will be activated using the device user's NMCI email account. A rescue account can be established utilizing a personal email account for the purpose of retrieving forgotten passwords.

7. User Reference for Mobile Device Management (Smartphone - IOS/Android)

a. The following chart provides some key "Do's" and "Don'ts" for Smartphones users, and the latest guidance and information updates can be found at the homeport link: https://www.homeport.navy.mil/services/mobile.

DO's	DON'Ts
DO download apps from approved locations (e.g. Apple App Store).	**DO NOT** conduct DoD sensitive work on the unsecured (native) portion of the device.
DO disable features such as Global Positioning System (GPS) and Siri when they are not in use. Outlook Web Access (OWA) or like connections to externally facing web-sites are authorized.	**DO NOT** physically connect any device to the Navy Enterprise (e.g., desktop computer or laptop).
DO set the internal clock to automatically update.	**DO NOT** remove the mobile device management (MDM) profile from your device.

DO disable AirDrop. At the time this must be user enforced (see below for instructions).	**DO NOT** connect your iOS mobile device to a Navy Marine Corps Intranet (NMCI) seat even for the purpose of charging. This will result in a security violation.
DO create an Apple ID (used for iTunes, App Store, and iCloud). iCloud is only approved for find my iPhone/iPad only.	**DO NOT** contact the service carrier or device manufacturer for technical support. Open a trouble ticket with the Electronic Serial Number (ESD).
DO remember your device passcode. The NGEN Systems Administrators cannot reset this passcode. The device will have to be wiped and all data will be lost.	**DO NOT** accept any iOS updates on your device until instructed to do so (refer to troubleshooting /problems section).
Do make sure your device is fully charged prior to installing an iOS or government furnished equipment (GFE) update.	**DO NOT** download apps with someone else's Apple ID; this will cause problems later.
Do set the internal clock to update automatically (settings, general, date & time, set automatically).	**DO NOT** copy and paste data outside the secure container.
Do follow DoD and DON Policy regarding the use of Bluetooth devices.	**DO NOT** name the device with something that exposes any affiliation with the DoD (e.g., AFSPC/CC iPhone).
	DO NOT remove any security measures as it could put the Navy Enterprise at risk, resulting in administrative or legal action.

b. Smartphones and Tablets **are not** to be connected via the Universal Serial Bus (USB) port for your NMCI or OCONUS Navy Enterprise Network (ONE Net) computer for the purpose of device

battery charging.

c. **DO NOT install iOS updates** until told to do so by a Navy Enterprise authority (e.g. NETOPS as this may cause the device to become temporarily unusable).

d. As with other WDs, lost and stolen Smartphones/iPADs must be properly reported to the store front manager or WD.

8. Forms and Reports. All forms and policy guidance related to cellular phones and wireless management are located at the following link https://g2.cnic.navy.mil/tscnichq/N6/N65/WSM/default.aspx.

9. Equipment Exchange. Recycling old wireless devices and accessories through third parties is not authorized. WD Managers are only authorized to "exchange" wireless equipment from wireless carriers as permitted by the DON wireless contract. Wireless equipment exchange only permits the acquisition of like equipment or the exchange of non-surplus/obsolete equipment and will not be used for services or be conducted with vendors not authorized by the DON wireless services contract.

10. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

D. R. SMITH
Vice Admiral, U.S. Navy

Distribution:
Electronic only, via CNIC Gateway 2.0
https://g2.cnic.navy.mil/CNICHQ/Pages/Default.aspx