ROY COOPER
ATTORNEY GENERAL

State of North Carolina

Department of Justice
PO Box 629
Raleigh, North Carolina
27602

October 1, 2013

Chairs, Joint Legislative Oversight Committee on Information Technology

North Carolina General Assembly
Legislative Building
16 West Jones Street
Raleigh, NC 27601

Re: Department of Justice Mobile Device Report

Dear Members:

Pursuant to Section 7.18(b) of S.L. 2013-360, please find the attached report from the Department of Justice on mobile electronic communication devices. As requested, a copy of the Department's policy on use of mobile communication device is included.

Thank you for the opportunity to provide this information. We would be happy to respond to any questions you may have regarding this report.

Very truly yours,

Kristi Hyman
Chief of Staff

KH/ml

cc: Chris Estes, NC Chief Information Officer
NCGA Fiscal Research Division

SUMMARY OF CELLULAR PHONE/MOBILE DEVICE COUNTS & EXPENSES
NC DEPARTMENT OF JUSTICE, October 1, 2013

	2012	2013		
Type of Device	Number of Devices		Average Monthly Cost	Annual Expense
Voice Only Phones	214	96	$ 28.84	$ 33,224
Air Cards	66	79	$ 38.97	$ 36,944
Tablets	48	69	$ 38.97	$ 32,267
Smartphones	211	342	$ 49.27	$ 202,204
Total Devices	539	586	$ 44.08	$ 304,638

Notes:
All mobile communication devices obtained for the Department of Justice are through the ITS state contract.
The cost of devices for the Department of Justice since the last report (October 2012) has decreased from $306,261 to $304,638.

NORTH CAROLINA DEPARTMENT OF JUSTICE

TO: North Carolina Department of Justice Employees

FROM: Nels Roseland, Chief Financial Officer

SUBJECT: Agency Cellular/Mobile Device Usage Policies

DATE: September 30, 2011

I. PURPOSE

The purpose of the Cellular/Mobile Device Usage Policies is to provide direction and guidance to all sections in the agency for the management of cellular/mobile devices and related services. These devices include cell phones, personal digital assistants (PDAs), smartphones, tablets, mobile broadband devices (such as Air Cards), associated accessories, etc. Related services include device service plans, push-to-talk, and global positioning systems (GPS). These policies conform to applicable state and federal policies and requirements. Lastly, Division managers may institute more stringent internal control procedures related to mobile devices, however in the event of a conflict these DOJ agency policies shall take precedence.

II. FOR ALL AGENCY OWNED AND ASSIGNED CELLULAR/MOBILE DEVICES

1. All Agency-Assigned Cellular/Mobile Devices, also known as Mobile Devices, must be:

   a. Procured via ITS state term contracts or through a related state approved procurement process,
   b. Only issued to employees based on a critical requirement for job performance. Written justification is required and must be maintained by the Agency and reviewed annually,
   c. Used in accordance with Office of State Budget and Management (OSBM) Policies in the OSBM Budget Manual, under "Mobile Communication Device" and "Telephone Calls",
   d. For government business use only,

e. Issued to employees when more economical means of telephoning are not reasonably available, and

f. Secured using a personal identification number (PIN) or other password protection. Automatic lockout must be enabled for 5 or fewer minutes of inactivity.

2. Employees are responsible for:

a. Ensuring that all usages (e.g. phone calls, texting, web browsing, e-mail access, etc.) made to or from their Agency-assigned Mobile Device are business related. Non-business uses are prohibited, except in emergency circumstances or in unpreventable instances where the user has no ability to control. In cases of unofficial incoming calls or message, the duration should be minimized once it is evident the usage is non-business related.

b. Mobile devices are to be used in a proper and safe manner. Because of safety risks, using state issued mobile devices while driving a motor vehicle is not recommended. Texting while driving is prohibited by state law, except for employees who are sworn law enforcement officers who are performing official duties.

c. If a state issued device is lost or stolen, employees must inform their supervisor and the IT Division Customer Support Center (CSC), ATTN: Mobile Device Administration, at csc@ncdoj.gov, as soon as possible. Employee should also report to CSC if the Mobile Device becomes infected with a virus/malware.

d. Employees who are assigned state owned devices are to be informed that they have no expectation of privacy for call activity or transaction activity that occurs with the device. Data contained on the device may be designated as public records.

3. Employee Personal Use:

a. Emergency use of the Agency-assigned Mobile Device for personal calls or messages shall include circumstances which have a direct effect on the health, safety and/or well being of the employee or their immediate family. It also includes calls or messages made to the employee's residence to inform someone that the travel period has been extended beyond the original plans due to unforeseen circumstances. These uses should be limited in frequency and duration.

b. If unforeseen circumstances result in an employee making non-emergency personal use of the Agency-assigned Mobile Device, the employee shall notify their supervisor and reimburse the Department of Justice for personal use activity. Personal use activity may include non-business use of email accounts, cameras or recording applications, text messaging, gaming applications, social media and other activities.

c. Any charges from content providers (such as iTunes, Android Market, etc.) to the Agency-assigned Mobile Device will be the responsibility of the employee, not the Agency, unless approved by the Agency prior to purchase. Employees may also be required to remove files or applications that have not been approved by the employee's supervisor.

d. Employees who use state owned devices for personal use are required to reimburse the state at a minimum rate of $0.25 per minute or $0.25 per personal transaction (e.g. texting, messaging or similar transactions). If DOJ monthly bill statements include charges for downloaded applications the employee will be required to reimburse DOJ for the actual costs specified on the monthly bill. Reimbursement payments shall only be paid by personal check or money order and be made payable to "North Carolina Department of Justice."

e. Willful, intentional misuse of an Agency-assigned Mobile Device shall be reported by the supervisor by way of a written memorandum to the agency Division Directors or Managers with additional copies designated to the Financial Services Section.

f. A pattern of willful, intentional misuse of an Agency-assigned Mobile Device shall subject an employee to disciplinary action as outlined in the State Personnel Manual.

4. Supervisor Responsibility:

a. Supervisors shall be responsible for ensuring prompt notification to the Information Technology Division, Customer Service Center for reassignment of any Agency-assigned Mobile Devices within their division/district/section/unit. This notification shall be made by memorandum or e-mail to the CSC@ncdoj.gov.

III. AUDIT AND JUSTIFICATION PROCESS

Cell phone and Mobile device usage is subject to audit and review by the State Auditor's Office, DOJ Internal Audit Office, DOJ Financial Services Section staff, DOJ Information Technology Division staff and by employee supervisory and managerial personnel.

Audits conducted by above noted parties may include random, unannounced reviews of Cellular/mobile device bills to determine compliance with applicable guidelines and the appropriateness of the calling plan. At least annually, each employee's job duties will be evaluated to make the appropriate determination on assignment of a state issued mobile device or payroll related cellular device allowance. The critical need to respond to an emergency or time sensitive criminal justice or legal service related issue shall be considered in the annual justification.

a. Annual Justification Statement - To memorialize the review and to ensure employees understand these policies and procedures, each Division Director/Supervisor shall complete and sign a MOBILE DEVICE JUSTIFICATION STATEMENT. This STATEMENT must be reviewed and signed annually by the employee and supervisor by the second Monday of each December. A signed copy of the form shall be emailed to Payroll@ncdoj.gov or faxed to (919) 716-6751. The Department reserves the right to de-activate or cancel the mobile device service from an employee for non-compliance.

b. Access to Records for Auditing Purposes - The State Auditor, DOJ IT staff, DOJ Financial Services staff and DOJ internal audit staff shall have unrestricted access to any and all records, physical properties and personnel associated with mobile device monthly bill statements, call records and related device information.

c. Release of Confidential Audit Related Workpapers - Records compiled by the SBI are confidential in accordance with Chapter 114 of the North Carolina General Statues. In accordance with N.C.G.S. § 132-1.4, records of criminal investigations and records of criminal intelligence information are not public records. Any information (verbal or written), documents, materials of any description, provided to DOJ Internal Audit staff, the State Auditor or DOJ IT staff related to an audit of SBI mobile device bill statements or call records may be considered confidential records of criminal investigations and/or criminal intelligence information.

d. Safeguarding of Records - Due to the sensitivity of the information reported in these records, access to any records related to such mobile device activity should be limited to authorized personnel at the SBI, DOJ FSS, DOJ Internal Audit staff and DOJ IT division staff. All records should be kept in a safe and secure place. With respect to information requests from external third parties, DOJ mobile device billing records, call logs and related information shall not be released to external parties unless the information is reviewed and approved by the Chief Deputy Attorney General or the General Counsel to the Attorney General or their respective designated attorneys.

IV. MOBILE DEVICE-SPECIFIC POLICIES

1. CELLULAR PHONES

a. Agency support for Mobile Devices is through carriers (e.g. Verizon Wireless) for any device with cellular wireless service plans. Contact ITD CSC, ATTN: Mobile Device Administration, for assistance.

2. SMARTPHONES OR TABLETS

a. Laptop and computer use policies apply to this Mobile Device policy.

b. Agency support for these Mobile Devices is through carrier support (e.g. Verizon Wireless) for any device with data service plans. Limited IT Support is available only for integration with Agency Information Technology (IT) Services. Contact ITD CSC, ATTN: Mobile Device Administration, for assistance.

c. Employee is responsible for data backups in a secure fashion.

d. If agency-assigned Mobile Device is to be connected to the Agency JUSTICE network, use Agency IT Service, and/or store Agency data then CJIS and ITS Information Security policies apply:

1) Run antivirus/ anti-malware software (if available for Mobile Device),

2) Subscribe to remote wipe and remote locator service.

3) Engage encryption with Agency-approved encryption technologies (if available for the Mobile Device); required if storing Agency data,

4) Use strong passwords with phone/ tablet-lock feature.

5) Turn off Bluetooth and Wi-Fi options by default. If in-use, these must be configured in a secure mode (not in "open access" or "discovery" setting).

6) Secure Mobile Hotspot configuration if utilized (not in open access mode).

e. Installation of non-Agency provided mobile apps, even if free, could violate the above security policies. Agency will not provide support for any mobile app unless part of the Agency IT Services, listed below. Employee should contact their supervisor for approval before purchasing or downloading any mobile app.

3. MOBILE BROADBAND DEVICE

a. CJIS and ITS Information Security policies apply. These are available on the Agency's Intranet web site.

b. Employee should ensure air time minutes do not exceed the contracted cellular data plan.

4. TECHNICAL ASSISTANCE

If employees have questions or need technical assistance about these policies they should send an email to csc@ncdoj.gov or call the ITD help desk at (919) 773-7900.

V. EMPLOYEE-OWNED MOBILE DEVICES

1. Employee is permitted to use his/her own Mobile Device for Agency related business under the following policies:

a. Employee can connect to Agency's Wi-Fi network as long as usage of the network complies with state and department related acceptable use policies. Do not connect device to any desktop or laptop computer on the Agency network.

b. Employees who store agency data on their employee owned devices are responsible for ensuring the agency data and information is secure, which includes e-mail attachments.

c. The employee, as owner of the Mobile Device, is responsible for the security, backups, and service of the Mobile Device, not the Agency. The Mobile Device is not supported by the Agency.

d. Information Security Guidelines in using the Mobile Device:

1) Run antivirus/ anti-malware software (if available for Mobile Device),

2) Subscribe to remote wipe and remote locator service.

3) Engage encryption with Agency-approved encryption technologies (if available for the Mobile Device),

4) Use strong passwords with phone/ tablet-lock feature.

5) Turn off Bluetooth and Wi-Fi options by default. If in-use, these must be configured in a secured option (not in "open access" or "discovery" mode).

6) Secure Mobile Hotspot configuration if utilized (not in open access mode).

e. If subscribed to an Agency IT Service, employee is aware that such services are voluntary and the Agency is not responsible for the potential deletion of any personal data if a remote wipe or configuration process is utilized. Owner is to perform the remote wipe procedure when required, since the Agency does not own the Mobile Device.

VI. AVAILABLE AGENCY IT SERVICES FOR MOBILE DEVICES (INCLUDES AGENCY OWNED DEVICES AND EMPLOYEE OWNED DEVICES)

a. Microsoft Exchange messaging via Exchange Active Sync: remote configuration and remote wipe.

b. Encrypted VPN into Agency JUSTICE network.

c. Agency Wi-Fi system Access.

d. Agency-supported Mobile Device for these IT Services: List of supported Mobile Devices is located on the Agency's Intranet web site.

e. Copies of agency issued phone statements and call logs may be provided by ITD staff and may be requested by sending an email to csc@ncdoj.gov. These monthly statements may be provided to the employee issued a state owned device, their supervisor and DOJ financial staff and DOJ Internal Audit and contracted agents.

VII. DEFINITIONS

a. Agency: North Carolina Department of Justice

b. Agency Data: information, records, or metadata created and processed by the Agency and ownership by specific Agency section(s) or division(s). The data could be public record, sensitive, or confidential.

c. Bluetooth: short-range wireless technology standard for exchanging data from fixed or mobile devices, creating personal area networks. Typical use is a Bluetooth headset connecting to a cellular or Smartphone.

d. Cellular Phone: Cellular phones are battery powered telephones requiring the cellular wireless network and associated service plans from Verizon Wireless, AT&T, etc. No data (Internet) connection is available with these mobile devices, only voice and texting services available. These phones may have additional memory, sometimes removable called an SD Card, to store photos and other files, and could be connected to a computer via USB cable.

e. Criminal Justice Information Systems (CJIS): FBI law enforcement data processing system. NCDOJ provides core connectivity for all NC law enforcement agencies to CJIS.

f. CSC: NCDOJ IT Division Customer Service Center, formerly the IT Helpdesk.

g. Employee-Owned Mobile Device: the mobile device was purchased or leased by the employee and not by the Agency.

h. Guideline: an official recommendation indicating how something should be done or what sort of action should be taken in a particular circumstance.

i. ITS: North Carolina Information Technology Services

j. Mobile App: Mobile software Applications for smartphones and tablets

k. Mobile Broadband Device: mobile data cards, including Air Cards and USB wireless modems. GPS with external network access would be included in this definition.

l. Mobile Hotspot: also known as tethering, the ability for the Smartphone or tablet to share the Internet connection with other devices nearby.

m. PDA: Personal Digital Assistant, typically without telephone service, such as the Palm.

n. Policy: course of action adopted by the Agency or the set of principles, regulations, or rulings on which they are based.

o. Smartphones: Includes "feature" web-browser-enabled cellular phones.

p. Strong Password should:

    i. Be a minimum length of eight (8) characters on all systems.

    ii. Not be a dictionary word or proper name.

    iii. Not be the same as the User ID.

    iv. Expire within a maximum of 90 calendar days.

    v. Not be identical to the previous ten (10) passwords.

    vi. Not be transmitted in the clear outside the secure location.

    vii. Not be displayed when entered.

q. Tablets: or tablet computer, includes Apple iPad, Motorola Xoom, Samsung Galaxy Tab, and others, utilizing a flat touchscreen.

r. Texting: also known as Short Message Service (SMS) or text messaging, refers to the exchange of brief messages between mobile or fixed (e.g. PCs) devices.

s. USB: Universal serial bus

t. VPN: Virtual Private Network

u. Wi-Fi: Wireless Fidelity or wireless local area network. Typically, no service fees are charged for Wi-Fi access, in comparison to cellular wireless services.