Email regarding the use of iPhones and Androids within the Enterprise. Received from: Dan Q. Bradford on Monday 29 August 2011.

Ladies and Gents,

As the Army Enterprise DAA, let me clarify where we are on mobile devices, including the i-Series of devices from Apple. First, I can assure you that I and other senior leaders in the Army want the capabilities these devices offer in the hands of our soldiers and warfighters just as much as you do. However, as mentioned below, there is an IA and O&M component that must be addressed to permit use.

Specifically:

I am required to enforce the following items on ALL mobile devices before we can add them to the network; the DoD and Army CIOs hold me accountable for these items. This includes Apple and Droid-based devices. The only way I can add mobile devices to Army's network is if the DoD and Army CIOs relax the following requirements:

1. FIPS certification from NIST (anything involving an encryption module or algorithm requires FIPS 140); it can't be waived - DoD requirement.

2. CAC/PKI so we can sign and encrypt email traffic as well as provide 2-factor authentication for the devices.

3. Data Encryption at Rest (DAR). Whole disc encryption is required to protect data on the device.

4. Enterprise Policy Management server so we can see, patch, and lock down mobile devices, like we do the desktops. The Blackberry Enterprise Server (BES) is an example of this. Apple doesn't have one that's fielded yet. I did see something promising at the LWN conference, but there's not an Enterprise instance yet.

5. Support package so we can O&M the devices/software, obtain tech support, and obtain software updates.

We have been working with Apple for several years in order to get desktops and mobile devices compliant so we could add them to LandWarNet (LWN). However, I still don't have everything I need so that I can accredit devices/OSs, assess risks, and move forward, permitting you to use mobile and desktop platforms from this vendor. I am much closer with the Apple desktops than I am with the mobile platforms. I think the Droid platforms are in about the same boat as Apple or even behind them.

Apple mobile devices, including iPhones and iPads still don't have items 1-5 above. I believe Apple submitted their iOS v4 (OS that drives the iPhone and iPad) for FIPS certification several months ago. I was notified that they pulled it back and are now resubmitting their iOS 5 for FIPS. They are just clearing commercial lab testing and have yet to submit those results to NIST in order to begin the process. In my humble opinion, that means they are at least 9-12 months out on any FIPs approval for their mobile iOS (given current DoD and NIST processes in this area). At this time, I do not know if iOS 5 will have a CAC/PKI and DAR solution included as part of this certification. If iOS 5 does not include this, the certification of the OS itself won't help me put it on the network. Third party solutions would be acceptable.

So bottom line is:

1. Mobile devices from Apple or other vendors cannot be legally added to LWN until they are able to meet items 1-5. The only one that can currently do this is RIM with their Blackberry devices.

2. I haven't spoken about mobile apps, but DoD and Army need to figure out how and where to host Army approved mobile apps. The CIO/G6 is working this issue.

3. Dual persona is something users want (ability to use a device for personal and Govt use), but this varies by manufacturer and device. The CIO/G6 would need to issue policy and guidance on dual persona in the Army.

4. Lastly, I must verify current policy in regard to DoD's TAA requirement (speaks to the manufacture of devices in the USA and not off-shore) - I believe the only machines Apple currently manufactured in the USA are the iMACs and Mac Pro's (I'm told the Mac Pro will be discontinued - haven't verified it). The other devices, such as iPhones, iPads, and MAC Book Pro's are apparently made off-shore (China, I believe - maybe other locations).

Lastly, we're working with many vendors to push them towards compliant devices and OSs so that we can take advantage of the same features, mobility, power, and flexibility that you enjoy on your personal devices. We just want to use them in a secure and supportable fashion to protect the data that's going over them. We want the innovation and technology that Industry can give us, but we also desire the security that must accompany such innovation.

v/r

Daniel Q. Bradford
Enterprise DAA