To: Steven Dayhoff
FCC Application Processing Branch

From: Norm Shivley, Meteor Communications Corporation

Re: FCC ID BIB6100000-01

Applicant:	Meteor Communications Corporation
Correspondence Reference Number:	29535
731 Confirmation Number:	EA387748
Date of Original E-mail:	09/02/2005
Date of Response:	09/13/2005

The following is a response to your 9/2/2005 list of questions received via e-mail. Answers are written in boldface type.

On 9/2/2005 you wrote:
The following items should be addressed for all SDR filings. In the following discussion, software includes firmware or any components in the memory modules which are used for control the RF performance of the transmitter without changes to its hardware.

1. Indicate how the software updates are implemented, distributed and controlled. Describe how the unit meets the overall requirements of 2.932 (e) for software download and authentication, and as appropriate, the following questions need to be addressed.

See section on Software Updates in amended Exhibit 3.

o For example, are only new units modified/updated prior to shipment?

MCC plans to be able to modify/update both old and new units.

o Are units that are already sold updated through the installation of a new end user installed driver for the new configuration?

Yes, the SDR software will be updated from time to time with new drivers. This update and software authentication process is described in amended Exhibit 3, Section 3 titled Authentication of SDR OS and DSP SW Drivers.

o If the end user updates the new configuration with a new driver, how do you ensure that only authorized driver is used with the proper device?

The update and software authentication process is described in amended Exhibit 3, paragraph 3.8.

o Describe what means exist to prevent the end user modifying the software, driver or memory through a patch mechanism or other means which may modify the approved software?

Unauthorized modification of software drivers change driver image and as such change the calculated security Certificate. As a result this calculated certificate will not match the embedded certificate (stored inside the original driver image) and the

driver will be rejected. For additional detail, refer to the amended Exhibit 3, Section 3.

o What authentication or security system measures are there to ensure that no third party can modify the software portion that controls the RF parameters?

MCC uses a Certificate system that is used to validate every driver image. See section on Authentication in amended Exhibit 3 for additional detail.

o Indicate how the software access is controlled and what 3rd party changes are permitted which may change the RF characteristics of the device.

MCC does not distribute its source code outside of MCC's Engineering Department. This prevents third party changes to code that would change the RF characteristics of the radio outside the bounds of the Certification grant.

The binary download files (used to update software) are also controlled by MCC and released to authorized customers only. Downloads to the radio require the use of MCC's XTERM software which requests a unique KEY in order to complete the download. This prevents the copy and use of download files by unauthorized users. The Keys are also strictly controlled.

o How does the hardware or existing software verify that only authenticated software is operating in the system?

Prior to loading software into the DSP, a verification process is performed. This process runs every time the radio is power cycled or loaded with new software. See the Authentication section of the amended Exhibit 3 for details.

o If the hardware with software control has the ability to operate in multiple regulatory domains, what control exists that while in US only the authorized software is capable of operating? (i.e. how does the system prevent a European version of the software running in US?

At this time there is only one regulatory domain version of software authorized to run in the SDR. It is the US version. In the future radios sold and operated in the US will only verify and authenticate with US approved formats. Radios sold and operated in Europe will only verify and authenticate with European approved formats.

2. How can the FCC verify, in the field, that correct version of the software is running in the device?

The FCC can connect to the radio operator port, and using a terminal emulation program (such as ProComm or HyperTerminal) read out the SW part number, rev number, and checksum. MCC publishes authorized SW part numbers along with checksums on its web site. See amended Exhibit 3, paragraph 3.6 through 3.10 for additional detail.

o Submit a description of this capability and instructions for the FCC to use in the field to verify that proper software is operating in the device.

1. **Connect a laptop computer to the operator port (RS-232) of the SDR (laptop must be able to run a terminal emulator program (ProComm or HyperTerminal or MCC's own XTERM)**

2. **Start the terminal program. Set baud rate to 9600 8,N,1, no hardware flow control.**

3. **Issue the following command: REV**

"REV" command example print out:

```
-------------------------------------------------------------

REV 09/08/05  16:58:00

           MCC-6100 SDR PACKET DATA RADIO
(c) Copyright 2005 Meteor Communications Corp.
            All Rights Reserved
S/W Part Number P1101-00-00 MCC-6100 SDR Version 1.05 08/31/05
(Checksum) (Byte count)

-------------------------------------------------------------
```

4. **Issue the following command: DSP**

"DSP" command example print out:

```
-------------------------------------------------------------

dsp 09/08/05 16:58:09

Active DSP image is: 050619a sdr2.out     Checksum is: CAIC  Byte
Count: 046602

STORED DSP DRIVERS

DSP1: 050619a sdr2.out (Checksum)(Byte count)
DSP2: 050701a sdr2.out (Checksum)(Byte count)
DSP3: Image is not assigned

-------------------------------------------------------------
```

o Are there any means by which software version numbers can be related to any future Class III permissive changes?

No.

3. A high level (simplified) block diagram of the software architecture should be submitted as an exhibit.

See the amended Exhibit 3 Section 6.

4. Additional information on authentication of the software is needed. When different drivers are available, how does the device ensure that the provided driver to the end user will be compliant? The end user must not be able to install drivers that can operate the device with unapproved radio parameters or modes.

All released software is tested at MCC to verify compliance before distribution to the field. Only MCC can compile valid object code. The device ensures only valid code is loaded using the Certificate verification method described in amended Exhibit 3, paragraphs 3.2 and 3.3. Therefore, only compliant code can be loaded into the device.