Date: February 5, 2015

Federal Communications Commission
Office of Engineering and Technology Laboratory Division
7435 Oakland Mills Rd.
Columbia MD 21046

Attn: Office of Engineering and Technology

Subject: Attestation letter regarding UNII client device without radar detection capability

FCC ID: BCGA1489, Model A1622, A1623

These devices do not support Ad-Hoc / Wi-Fi HotSpot mode in Wi-Fi 5 GHz band.

In AirPlay mode, these devices do not initiate transmission of any probes, beacons and do not initiate Ad-Hoc operations when not associated with and under the control of a certified master device, according to Section 15.202 of FCC rules.

Future changes to any Apple Operating System used in these devices will not change the DFS operational characteristics, in any mode of operation.

Software security questions and answers per KDB 594280 D02:

Section	Questions	Answers
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The software/firmware update is bundled, as part of the iOS software update, and the user or installer cannot modify the content. The installation and/or update proceeds automatically once the user accepts to install/update the software/firmware.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release is verified by the Grantee before release. If required, Grantee will follow FCC permissive change procedure.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	Yes, software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.

Apple Inc.
1 Infinite Loop
Cupertino, CA
www.apple.com

	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Yes, see answers to #1 and #3.
	5. Describe, if any, encryption method is used.	Yes, encryption using proprietary internal software.
	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as a master in some band of operation and client in another; how is compliance ensured in each band of operation?	Not applicable, this device is a client-only device.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	Only Grantee can release or make changes to the software/firmware using proprietary secure protocols.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	No, refer to the answers #1, 2, and 3 under General Description.
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	No, refer to the answers above.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Grantee proprietary hardware platform, software tools and proprietary protocols are required to replace firmware.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	Not applicable, this device is not a module.

Sincerely,

Tiberiu Muresan
Apple Inc.
Wireless Certification Manager
tmuresan@apple.com