HwaCom Systems Inc.

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21048

2015-7-29

Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices close DFS Frequency Band

FCC ID: **2AE4C-M210**

This device does not support Ad-Hoc/WiFi Hotspot mode in in WiFi 5GHz band.
This device will close UNII Band 2A and UNII Band 2C when sells in USA and 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. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.	The software/firmware update is bundled; the user or installer cannot modify the content. The installation and/or update proceeds automatically once the user accepts 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. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification	Yes, software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is	Yes, please see answer 1 and answer 3

	legitimate	
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	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 master in some band of operation and client in another; how is compliance ensured in each band of operation?	Not applicable, this device will only operate non-DFS band.
Third-Party Access Control	1. 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.	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 answer 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, please refer to the answers above.
	4. What prevents third parties from loading non-US versions of the software/firmware on the	Grantee proprietary hardware platform software tools and proprietary protocols are required to replace firmware.

	device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT	
	5. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization.	Not applicable, the device is not a module.

Sincerely

Jack Chen

(signature)
Name and Title: PM
Company Name: **HwaCom Systems Inc.**
Address: 11Fl., No.108, Sec. 1, Hsin-Tai-Wu Rd., Hsi-Chih District, New Taipei City 221, Taiwan, R.O.C.
E-mail: jack.chen@hwacom.com
Telephone: 886 988 309 282
Fax: 02-26967199