<Dongguan Digital AV Technology Corp., Ltd.>

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

<2016-03-22>

Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices

FCC ID: 2AGM4-WUS13

Software security questions and answers per KDB 594280 D02:

Software Security description – 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 user cannot download software/firmware, because the software upgrade is not support for the end user.
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?	The radio frequency parameter store in non-volatile memory (EPROM) and it cannot be modified by end user except our professional service engineer used special tools and drivers.
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	The devices radio frequencies were controlled by the radio frequency parameter which store in non-volatile memory (EPROM). If the radio frequency parameter missing the radio frequencies will not working anymore. And the radio frequency parameter needs special tools and drivers to re-flesh.
4	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	The user cannot download software/firmware, because the software upgrade is not support for the end user.
5	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	The radio frequency parameter was produced by special software after calibrated. And the radio frequency parameter packed encrypts used Message Digest Algorithm MD5

		method.
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?	The radio frequency parameter was produced by special software after calibrated. And the radio frequency parameter packed encrypts used Message Digest Algorithm MD5 method.
Software Security description – 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.	No, there is no body can re-flash the radio frequency parameter except our-self.
2	Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.	The user cannot download software/firmware, because the software upgrade is not support for the end user and third parties.
3	For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization.	Our devices software drive was design by our company, and will not public to end user.
Software Security description – USER CONFIGURATION GUID		
1	Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.	The UI for the end user only can selected the channel list during operating, and these channel lists are authorized in US/ Canada.
	a. What parameters are viewable and configurable by different parties?	The end user only authorized tune on/off radios, and 2.4G band 5G band mode selection and channel numbers which authorized in

		US/Canada.
	b. What parameters are accessible or modifiable to the professional installer? i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The professional installer only install the module driver and operating software, Cannot change the transmit parameters.
	c. What configuration options are available to the end-user? i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user can not accessible or modifiable any radio frequency parameters. The parameters can only be changed remotely within the limits of country code US. The country code and regulatory domain control do limit all the parameters set
	d. Is the country code factory set? Can it be changed in the UI? i. If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	No, there is no country code in factory set, the radio frequency parameter of this device is for in US/Canada use only, and the end user cannot change it. It cannot be changed.
	e. What are the default parameters when the device is restarted?	At each boot up the country code and the antenna gain are read from the non-volatile memory, those values are configured during module production.
2	Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.	No, this devices cannot be configured in bridge or mesh mode.
3	For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for	This device was designed only as a client without radar detection function. There for the end user cannot configure this device in the

	each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	end user UI.
4	For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. See Section 15.407(a).	No, it cannot configured as a AP.

Sincerely

(signed)
Name/Title: Qing Feng Zhang/Director of PM Dept
Company: Dongguan Digital AV Technology Corp., Ltd.
Address: 2nd floor F2-S3 district, No.18 Haibin road, Wusha, Changan Dongguan, 523860, China
Phone: (86) 769-86076999
Fax: (86) 769-86076938
Email: zqf@oppo.com