Huawei Technologies Co., Ltd.

Statement

Federal Communications Commission
Oakland Mills Road
Columbia MD 21046

2019-03-22

Industry Canada

Subject: Statement for 2.4G Wi-FiTM
FCC ID: **QISMACHR-WX9**
IC: **6369A-MACHRWX9**

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03.
The information below describes how we maintain the overall security measures and systems so that only:
1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

General Description	
1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.	There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in memory at the factory and cannot be modified or overridden by third parties.
2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	The Software/Firmware in the device, controls the following RF parameters: 1. Transmitter Frequency 2. Transmitter Output Power 3. Receiver Frequency 4. Channel Bandwidth 5. RSSI calibration The Software/Firmware controls the RF parameters listed above so as to comply with the specific set of regulatory limits in accordance with the FCC grants issued for this device. The RF parameters are limited to comply with FCC rules and requirements during calibration of the device in the factory. Security keys (certification certificates) are in place to ensure that these parameters cannot be access by the User and/or a 3rd party.
3.Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail	The firmware is programmed at the factory and cannot be modified by third parties.

how the RF-related software is protected against modification.	
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The firmware is programmed at the factory and cannot be modified by third parties therefore no encryption is necessary.
5. 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?	This is a client module only.
3rd Party Access Control	
1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.	3rd party does not have the capability
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.	3rd party does not have the permission
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.7	Not applicable – this is not a modular device
SOFTWARE CONFIGURATION DESCRIPTION	
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.	No UI provided.
a) What parameters are viewable and configurable by different parties?	None.
b) What parameters are accessible or modifiable by the professional installer or system integrators?	None.
i)Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without

	receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant).
c) What parameters are accessible or modifiable by the end-user?	None.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant).
d) Is the country code factory set? Can it be changed in the UI?	Default country code is set in the factory and no UI is provided for modification.
i)If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Programmed for default mode which is always FCC compliant. Always set for default for all start-ups, resets, timeouts or other host or network events.
e) What are the default parameters when the device is restarted?	Always FCC compliant.
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.
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 each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	This is a client device.
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))	This device is not an access point.

Best Regards

Zhang Xinghai
EMC Laboratory Manager

Huawei Technologies Co., Ltd.
Address: Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, P.R.C
E-mail: zhangxinghai@huawei.com
Tel: 0086-0755-28970299
Fax: 0086-0755-89650226

**Wi-Fi is a trademark of Wi-Fi Alliance