HIVE
Centrica Connected Home
Millstream
Maidenhead Road
Windsor
Berkshire
SL4 5GD
UK

Federal Communications Commission 2017-11-20
Oakland Mills Road
Columbia MD 21046
Model：HCI001
FCC ID: WJHHCI001, IC ID: 21719-HCI001

Subject: Statement for 5G Wi-Fi™
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

Software Security Description – KDB 594280 D02v01r01 Section II	
General Description	
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The user or installer cannot modify the software/firmware content. FW version will only be deployed over the air. There are two main scenarios for this (1) When the user associates the device to their account, the platform pushes a new firmware version if available. (2) The cloud platform can push a new firmware version to the device when it is available
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?	WiFi channel area code ID is only set in factory, all RF parameters (include Frequency range, transmitter output power etc.) can not be access by the user.
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	Firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded. Firmware is also pushed as an AES encrypted file, where the AES key is shared with the device via a separate channel.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded.
5. Describe, if any, encryption methods used.	SSL / AES / Base64

HIVE
Centrica Connected Home
Millstream
Maidenhead Road
Windsor
Berkshire
SL4 5GD
UK

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?	Our device has two radios, one for 2.4G band and another for 5G band. When client mode is enabled, the working band also must be selected, and the master mode working on that band will be disabled automatically. When each mode is selected, the wireless driver will be configured with specific settings for selected mode to let it work in that mode
Third-Party Access Control	
1. How are unauthorized software/firmware changes prevented?	There is checksum information in firmware upgrade bin file and flash ROM.
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.	It is impossible to load device drivers
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, 3rd party have no the capability
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	No method is used. The RF parameters are not included in firmware. So it is not necessary to prevent third parties from loading non-US firmware version.
5. For modular devices, describe how authentication is achieved when used with different hosts.	This is not modular devices.

SOFTWARE CONFIGURATION DESCRIPTION	
1. To whom is the UI accessible? (Professional installer, end user, other.)	End user
a) What parameters are viewable to the professional installer/end-user?	1.Area network SSID
b) What parameters are accessible or modifiable to the professional installer?	No
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	End user cannot access to the parameters
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Firmware does not provide any interface to user to operate outside its authorization
c) What configuration options are available to the end-user?	End-user have not configuration options
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes

HIVE
Centrica Connected Home
Millstream
Maidenhead Road
Windsor
Berkshire
SL4 5GD
UK

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No
d) Is the country code factory set? Can it be changed in the UI?	Yes, No
i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	No
e) What are the default parameters when the device is restarted?	Same as factory set
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?	The device can be configured as master (WAC), but user cannot configure it. When the device act as master, the firmware follow a build-in config file which comply with compliance, but user cannot access to this config file.

Company Officer: Darrell

Telephone Number: 00447867395548

Email: Darrell.Harris@BGCH.co.uk