QNAP Systems, Inc.

2F., No. 22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221 Taiwan
TEL: +886-2-26412000 FAX: +886-2-26410555

Date: 2015-06-04

FCC ID: **2ACFN-QLIVEBOX**

Software Operational Description

We, QNAP Systems, Inc. hereby declare that requirements of QLivebox have been met and shown on the following question.

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.
	Description: (1) Obtain and download The firmware could be obtained at below link address: Web site address : http://113.196.50.107/boxtest/FirmwareRelease.xml (2) Install The product has provided user a WEB UI interface, with which user could upgrade new 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?
	Description: Two radio frequency parameters can be configured via UI: Channel and Channel Bandwidth. All above two parameters are limited as a pre-set list for user to select from UI.
	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.
	Description: The source is a read-only web page. And the web server is secured with firewalls. Besides, 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.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.
	Description: Firmware itself has a private checksum value and MD5 value inside. If

QNAP Systems, Inc.

2F., No. 22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221 Taiwan

TEL: +886-2-26412000 FAX: +886-2-26410555

	verified, and then it cannot be allowed to be upgraded.
	5. Describe, if any, encryption methods used.
	Description: SSL / AES / TKIP
	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?
	Description: 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?
	Description: RF parameter's pre-set values are fixed in the ROM and all software/firmware update are protected by checksum and MD5 value.
	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.
	Description: It is impossible. Because RF parameters, country and other parameters (related to device compliance) are permanent settings in the ROM.
	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.
	Description: It is impossible. Because the parameters of country, frequencies and etc. are permanent settings in the ROM.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?
	Description: All parameters indicating different countries are permanent settings in the ROM. The software/firmware itself doesn't contain these parameters and so it will not be affected by version of software.
	5. For modular devices, describe how authentication is achieved when used with different hosts.
	Description: The product is Access Point, not modular device.
SOFTWARE CONFIGURATION DESCRIPTION	

QNAP Systems, Inc.

2F., No. 22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221 Taiwan

TEL: +886-2-26412000 FAX: +886-2-26410555

USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other...)
	a) What parameters are viewable to the professional installer/end-user?
	Description: Both professional installer and end user can modify below parameters: Mode, Channel Bandwidth, Primary Channel, Channel, Transmit Power, Beacon Interval, Legacy Rate Sets, SSID, Security Type, but only within ROM pre-set authorized range.
	b) What parameters are accessible or modifiable to the professional installer?
	Description: Same as above.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Description: All above parameters have pre-defined range according to the certification test result. They are stored in the ROM and shown in UI, which not allow user to adjust beyond the pre-set value.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Description: All parameters (RF, Frequencies and etc.) indicating different countries are permanent settings in the ROM. So if a device is a product for US, it cannot be changed for another region.
	c) What configuration options are available to the end-user
	Description: Mode, Channel Bandwidth, Primary Channel, Channel, Transmit Power, Beacon Interval, Legacy Rate Sets, SSID, Security Type, but only within ROM pre-set authorized range.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Description: All above parameters have pre-defined range according to the certification test result. They are stored in the ROM and shown in UI, which not allow user to adjust beyond the pre-set value.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Description: All parameters (RF, Frequencies and etc.) indicating different countries are permanent settings in the ROM. So if a device is a product for US, it cannot be changed for another region.
	d) Is the country code factory set? Can it be changed in the UI?
	Description: It is factory set and cannot 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.?
	Description: All parameters (RF, Frequencies and etc.) indicating different countries are permanent settings in the ROM. So if a device is a

QNAP Systems, Inc.

2F., No. 22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221 Taiwan
TEL: +886-2-26412000 FAX: +886-2-26410555

	product for US, it cannot be changed for another region.
	e) What are the default parameters when the device is restarted?
	Description: The parameters that user latest saved in the UI.
	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.
	Description: Mesh mode is not supported. For bridge mode our device can only connect to the access point with specific SSID. Our device in bridge mode only performs a passive scan (listening only) without sending any packet out in the DFS channels. Our device will communicate with the access point after receiving beacon packet from the access point with specific SSID. If the access point detects radar signal and change to another channel, our device will follow the notification packet which indicates the new channel from access point's packet to change to the new channel that access point changed to. Our device acts in bridge mode cannot detect radar signal but just follow the base access point with specific SSID which is indicated in the bridge mode GUI.
	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 to ensure compliance.
	Description: User can only change channel for GUI, and GUI has limited the selectable channel, so user has no way to break compliance on our 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 section15.407(a))
	Description: These antennas (three PIFA antennas) are for Point to Multipoint only, and antennas are fixed internally and are not suppose to be changed by user.

If you should have any question(s) regarding this declaration, please don't hesitate to contact us. Thank you!

QNAP Systems, Inc.

2F., No. 22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221 Taiwan
TEL: +886-2-26412000 FAX: +886-2-26410555

Gask Huang / Application Engineer
Tel: +886-2-26412000 #11072
Fax: +886-2-26410555
E-mail: gaskhuang@qnap.com