TOPLINKST TECHNOLOGY COMPANY LIMITED.

SOFTWARE SECURITY DESCRIPTION (594280 D02 U-NII Device Security v01r03)

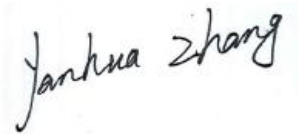
FCC ID: ZLJTOP-S5 Date:03/15/2017

General Description	
Q1	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.
Ans	We do not release the firmware on our website for downloading. We design and manufacture the device and end product by ourselves and the firmware from us will not be released to any external customer or manufacturers and it will be made available via secure server.
Q2	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?
Ans	Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory at the time of production. They will not exceed the authorized values.
Q3	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.
Ans	The firmware is installed on each single device during manufacturing process. The correct firmware is also verified and installed during manufacturing process. In addition, the firmware binary is encrypted using SHA-1 encryption and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated. The encryption key is known by ourselves only.
Q4	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
Ans	The firmware binary is encrypted, The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in non-volatile memory (see General Description Q3).
Q5	Describe in detail any encryption methods used to support the use of legitimate software/firmware.
Ans	Standard SHA-1 encryption is used.(see General Description Q3).
Q6	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?
Ans	The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band.

Third-Party Access Control	
Q1	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.
Ans	No
Q2	What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.
Ans	The embedded software is protected via the measures explained in the previous section(see General Description Q3). Distributions of host operating software are encrypted with a key.
Q3	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.
Ans	the device provide host control hardware or software interface to users, However, users can not change the frequency, power and other information, so that its internal RF parameters cannot be modified by outside the grant of authorization.

SOFTWARE CONFIGURATION DESCRIPTION

Q1	To whom is the UI accessible? (Professional installer, end user, other.)			
Ans	Not restricted. There is no user configuration GUI.			
	a)	What parameters are viewable to the professional installer/end-user?		
	Ans	The Hardware and software versions and IP addresses.		
	b)	What parameters are accessible or modifiable by the professional installer?		
	Ans	There is no user configuration GUI.		
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
		Ans	Yes.The values of the modifiable parameters are restricted toaspecific interval. There is no way to input a value beyond the authorized range.	
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
		Ans	No such controls.	
	c)	What parameters are accessible or modifiable to by the end-user?		
	Ans	The IP addresses.		
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
		Ans	Yes.The values of the modifiable parameters are restricted to a specific interval. There is no way to input a value beyond the authorized range.	
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
		Ans	No such controls.	
	d)	Is the country code factory set? Can it be changed in the UI?		
	Ans	Yes, the country code is factory set. No, it can not be changed in the UI.		
		(1)	If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	
		Ans	No such controls.	
	e)	What are the default parameters when the device is restarted?		
	Ans	Username/Password=admin/admin, HTTP port=80		
Q2	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			
Ans	Not applicable			
Q3	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?			
Ans	No end user controls or user interface operation to change master/client operation. The device is a master and cannot be configured as a client because of the hardware			
Q4	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))			
Ans	The product was controlled by software to ensure that the point to point or point-to-multipoint network architecture is under the same output power level and conform corresponding limit. The product use Printed antenna to ensure that users can not replace antenna.			



Client’s name / title : YanHua Zhang / Manager
Company Name: TOPLINKST TECHNOLOGY COMPANY LIMITED
Address: UNIT 04,7F,BRIGHT WAY TOWER, NO,33 MONG KOK ROAD, KOWLOON, Hong Kong
Phone: +852-27935511
Fax: +852-27935511
Email: zhangyh092@126.com