

Date: 2016-01-29

**SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES**  
**(594280 D02 U-NII Device Security 1.3, 11/12/15)**

**Company Name: SKY phone LLC**

**FCC ID: 2ABOSSKYELITE70**

**Product Name: 1348 Washinngton Ave. Suit 350 Miami Beach, FL33139**

<b>SOFTWARE SECURITY DESCRIPTION</b>	
<b>General Description</b>	
Q.	1. Describe how any software/firmware updates for elements that 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.
A.	Software can only be released through the company's website, download and login gateway to upgrade, The software/firmware update is not change the RF power levels frequencies etc.
Q.	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?
A.	RF parameter values cannot be changed where update software or firmware, the factory has been set to be less than FCC limits
Q.	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 how the RF-related software is protected against modification.
A.	Software versions has been encrypted by the manufacturer cannot be changed, so the RF parameter cannot be manipulated.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Encryption method has WEP,WPA-PSK(TKIP),WPA2-PSK(AES) & WPA-PSK(TKIP)+WPA2-PSK(AES), if want to change the product RF-related software/firmware, it must use the manufacturer 's key(6 digital password) to decoded.
Q.	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?
A.	When the product is used as the AP and ROUTER mode is the passive scanning, and as the repeater mode is active scanning, frequency range is 5150-5250MHz. The product configuration is cannot change the RF parameter.

<b>Third-Party Access Control</b>	
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.
	Software can only be released by our company to upgrade! Built in encryption chip
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 device is not permits third-party change the software or firmware installation.
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.
	Software is set at the factory on the hardware, the consumer can not modify the key parameters

<b>SOFTWARE CONFIGURATION DESCRIPTION</b>	
<b>USER- CONFIGURATION GUIDE</b>	
Q.	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.
A.	Consumers can access through the gateway, the user name and password landing router software display functions are open, will not touch any of the prohibition of the use of items.
	a. What parameters are viewable and configurable by different parties? <sup>9</sup>
	SSID, Channel, user login name, encryption mode
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	Power RF, the country's regional code is set at the factory, the other product name and encryption method, the channel is free to choose
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Factory when there is a fixed process, to ensure that no more than the authorized parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	As this situation, the user should assume corresponding responsibility when operate the device outside its authorization in the U.S.

Intracom Asia. Co., Ltd.

	c. What parameters are accessible or modifiable by the end-user?
	User name, SSID, encryption method, mode of product usage
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Our user's rights are only in accordance with their preferences to change UI, other relevant technical parameters can not be changed
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	When the user operate the device outside its authorization, the devices will be warnings and exit the operation interface automatic.
	d. Is the country code factory set? Can it be changed in the UI?
	Not
	e. What are the default parameters when the device is restarted?
	Keep the original settings
Q.	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.
A.	Not
Q.	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?
A.	When the device as s master or client, user is not permissive to enter into the UI to change RF parameter, and the RF parameter is preset by the manufacturer.
Q.	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.
A.	The device cannot use different types of antennas, so it is ensure sure that compliance with applicable limits and the proper antenna is used for each mode of operation.

Signature 

Company: SKY phone LLC  Sky Phone LLC  
 Title: Manager DEVICES FL US LLC Corp.

Name: Roberto Conrado  
 Address: 1348 Washington Ave. Suit 350 Miami Beach, FI33139