Company: Jiangsu SEUIC Technology Co.,Ltd.
Add: No23, Wenzhu Road, Yuhuatai District Nanjing, Jiangsu, China
Tel: 025-52261298-8101
Fax: 0086-25-52268995

SOFTWARE SECURITY DECLARATION FOR U-NII DEVICES
FCC ID: 2AC68-CRUISE1

SOFTWARE SECURITY DESCRIPTION	
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. RE: Update by system software or OTA webserver. The level of security are middle.
	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? RE: RF parameter is burned at factory, NO way can change parameters by users. Never allow the device to exceed the authorized RF characteristics.
	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. RE: The wireless devices are in accordance with 80211 WIFI standard and Bluetooth protocol. The RF-related software will not work when modification against standard or protocol.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. RE: Open,Wep40,wep104,wpa 802.1X,wpa2 802.1X,wpa-psk TKIP,wpa2-psk AES.
	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? RE: The wireless devices are in accordance with 80211 WIFI standard without DFS and compliance for related FCC rules.

Third-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. RE: No third parties or any manner have the capability to operate US-Sold device on any other domain, frequencies.
	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. RE: The wireless is in accordance with WIFI 802.11 and Bluetooth protocol. The RF parameters are in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, NO third-party functions to changed the firmware.
	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. RE: The manufacturers full comply with 802.11 standard. The parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.

SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	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. RE: The user configurations permitted through the UI. Different levels of access are not permitted for professional installers, system integrators or end-users.
	a) What parameters are viewable and configurable by different parties? RE: NONE
	b) What parameters are accessible or modifiable by the professional installer or system integrators? RE: NONE

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? RE: Yes
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? RE: The firmware is write in ROM. The end user cannot modify it.
c) What parameters are accessible or modifiable by the end-user? RE: NONE
i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? RE: YES
ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? RE: The firmware is write in ROM. The end user cannot modify it.
d) Is the country code factory set? Can it be changed in the UI? RE: Yes, No way can changed Country code.
i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? RE:NONE
e) What are the default parameters when the device is restarted? RE: The parameters is fixed for US, whatever the device is restarted or not
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. RE: 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? RE:YES, device support master and client. User configurations permitted through the UI. Hotspot acts as a master works in 2.4G band, Both master and client are accordance with WIFI 802.11 Standards.
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)) RE: Only support 2.4G WIFI Hotspot at 11g mode. No need proper antenna for other mode, and the device accordance with WIFI 802.11 standards

Client's signature: Keen Zheng
Client's name: Keen Zheng
Title: Manager