SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

In accordance with FCC KDB 594280 D02 v01r01, the new Software Security requirements for U-NII Devices, the following information is provided to describe the security features of the software in this device.

SOFTWARE SECURITY DESCRIPTION		
General Description	1 Describe how any software/firmware update will be obtained, downloaded, and installed.	Updates can only be obtained from FAE of SHC, Inc.
	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?	N/A
	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.	N/A, SHC release the OS / firmware to authenticated FAE.
	4 Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	N/A
	5 Describe, if any, encryption methods used.	to change setting of WiFi, need to administrator's password.
	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?	N/A
Third-Party Access Control	1 How are unauthorized software/firmware changes prevented?	to update software/firmware of WiFi, need to administrator's password.
	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.	No.
	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.	Not possible.
	4 What prevents third parties from loading non-US versions of the software/firmware on the device?	After SHC device is registered, device unique Serial number and regulatory domain are tied in to backend database to prevent third party fromdownloading non-US versions of firmware.
	5 For modular devices, describe how authentication is achieved when used with different hosts.	N/A

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	1 To whom is the UI accessible? (Professional installer, end user, other.)	UI can only be accessed through administrator's password authentication.
	a) What parameters are viewable to the professional installer/end-user?	No.
	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?	No.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No.
	c) What configuration options are available to the end-user?	No.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No.
	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?	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?	When device is restarted it will return to Factory setting.
	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?	N/A
	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))	N/A