microhard SYSTEMS INC.

150 Country Hills Landing N.W.
Calgary, Alberta T3K 5P3
Tel: (403) 248-0028
Fax: (403) 248-2762
E-mail: info@microhardcorp.com
www.microhardcorp.com

Leaders in Wireless Telecom

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

Applicant: Microhard Systems Inc
FCC ID: NS9VIP4GABGN20

June 15, 2016

To Whom It May Concern:

We attest the following regarding KDB 594280 D02 U-NII device Security

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.	There is no firmware provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in EEPROM memory at the factory and cannot be modified or overridden by third parties.
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?	There are no RF parameters that can be modified. All RF parameters are programmed in EEPROM memory at the time of production in the factory per FCC approved. These parameters are therefore fixed at the factory such that they will not exceed the authorized values.
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.	Yes. The RF Parameters is put in read-only partition of the memory and is only installed by the factory. RF Parameters will be locked in this partition.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The firmware is built at the factory and cannot be modified by third parties therefore no encryption is necessary.
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?	The device will be able as access point only ISM 2.4GHz band and UNII 3 bands. For compliance, device will transmit under approved power. And user can't access to change Master/client feature per band.
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.	No, third parties don't have capability to access and change radio parameters.

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.	RF parameters are programmed into EEPROM memory at the factory and cannot be reprogrammed or re-flashed by third parties. Also, device doesn't allow third-party 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.	Not a modular device

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.	The UI is accessible to anyone using the device. But the UI never gives access for specific RF parameters
a. What parameters are viewable and configurable by different parties?	Nothing to control the radio operation parameter for different parties
b. What parameters are accessible or modifiable by the professional installer or system integrators?	None.
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Some parameters are programmed in EEPROM, installer cannot access them. The system firmware is programmed and protected in flash memory. The installer/end-user cannot access the flash memory.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user has no access to configuration settings that could change the radio operation parameters.
c. What parameters are accessible or modifiable by the end-user?	End-user only can select approved channels and power levels on web UI, but cannot modify them.
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	
(2) What controls exist so that the user cannot operate the device outside its authorization in the	End-user only can select approved channels and power levels on web UI, but cannot modify them.

U.S.?	
d. Is the country code factory set? Can it be changed in the UI?	There is no country code factory set. Also, it couldn't be changed in the UI.
(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	It couldn't be changed. The end user has no access to configuration settings that could change the radio operation parameters programmed in EEPROM.
e. What are the default parameters when the device is restarted?	All of RF parameters are programmed into EEPROM memory at the factory.
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.	Yes, but it is operating in the frequency bands 5.745 to 5.825 GHz (UNII 3 bands range), not in DFS bands (5250-5350 MHz AND 5470-5725 MHz).
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?	For compliance, device will transmit under approved power. And user can't access to change Master/client feature per band.
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))	The device can be configured as an access point and client. Changing between access point and client can be done with the selection in the UI. There are regulatory parameters to limit product to operate the device under its authorization in the U.S. This regulatory parameters would define which channel would be available to operate in access point or client to meet UNII requirements.

Sincerely,

Hany Shenouda
Director of Engineering
Microhard Systems Inc