SOFTWARE SECURITY DECLARATION FOR U-NII DEVICES

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. The controller and AP upgrade images and Meru authorized Certificates are directly downloaded from the Meru support site and upgraded by the customer. The software verifies the controller license before upgrade.
	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) Operating Channel b) Channel width c) Transmit power (Maximum EIPR is limited by the regulatory limits. The Maximum EIPR limits are stored in the radio EMPROM. Customer can set low power only. d) RF mode (802.11a/b/n/ac) e) MIMO mode f) STBC support The above parameters are limited as per the regulatory requirements.
	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. The software/Firmware is downloaded with secured access to Meru support site. The software/firmware verification is done by md5 checksum, and meru specific secured mechanism.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. No Encryption methods used, just the signature.
	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 regulatory limits transmit power for each channel and modulation is stored in the radio EEPROM during the radio calibration at the manufacturing site. The country code is pre-set in the controller prior to shipping. The customer has no access to change the country code. The maximum power set in the AP is limited by the regulatory limit power in the radio EEPROM.

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. The Country code is set in the Controller prior to shipping. Customer has no access to change the country code or any other regulatory dependent parameters. The controller is licensed to the customer within US.
	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 does not permit third-party to change any software in the controller or access point. The controller is licensed and password protected. The firmware image is downloaded as a tar file. This file is untarred and MDS checksum verification done. The untarred contents contain a folder which contains all the PRMs to be installed. This folder contents are signed with a Meru signature (DSA) and this signature is verified on the controller after downloading the firmware image.
	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 Applicable

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.
	a) What parameters are viewable and configurable by different parties? Channel, power settings, antenna gain, country code.
	b) What parameters are accessible or modifiable to the professional installer or system integrators? Channel, power settings, antenna gain (for external antenna)
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? The operating channel and maximum transmit power are limited as per the country regulatory limit.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Country code is configured only during the installation and restricted thereon.
	c) What parameters are accessible or modifiable by the end-user? Operating channel, channel bandwidth and transmit power
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? The operating channel and maximum transmit power are limited as per the country regulatory limit. Installer cannot set higher than the authorized parameters.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Region Code is preset in the controller before shipping to the customer.
	d) Is the country code factory set? Can it be changed in the UI? The country code can be set during installation and is available for only professional installers.
	e) What are the default parameters when the device is restarted? Device configuration is stored internally and operates in the same configuration after restart.
	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

	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? No Scanning feature
	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 antenna gain is present in the controller. Only certified antennas are used.

Sincerely,

Rajendran V. Chary
Architect Hardware Development (USA)
899 Kifer Rd, Sunnyvale, CA 94086-5301
408-235-7700 X 81320

Dated: 06/09/2016