Software security requirements for U-NII devices

In accordance with FCC KDB 594280 D02 v01r03, a new software security requirement for U-NII devices, the following information is provided to describe the security features of the software on this device.

Software security description		
General description	1 Describe how to obtain, download, verify and install software/firmware updates for factors that may affect the device's RF parameters. For software accessed through the manufacturer's website or through the device's management system, the various levels of security are appropriately described.	It is bundled as part of a Software update, where user or installer cannot modify the content. When the firmware is produced by LGIT and distributed to the customer, the customer manages the firmware update of each terminal through the OTA server.
	2 Describe RF parameters modified by software/firmware without any hardware changes. Are these parameters limited in some way so that the device does not exceed the approved RF characteristics due to other software/firmware changes?	All RF parameters are hard-coded and validated before published. There are no way to change any RF parameters excepted for System software update.
	3 It details the authentication protocol in place to ensure that RF-related software/firmware is from valid source. Explain in detail how RF-related software is protected from modification.	RF-related software/firmware are included in a system software and validated before update. Before firmware update, you can get the check sum of the firmware and update only the legal F/W.
	4 It details the encryption method used to support the use of legitimate RF-related software/firmware.	Limit by checksum Before firmware update, you can get the check sum of the firmware and update only the legal F/W.
	5 For devices that can be configured as master and client (including active or passive discovery), please describe how the device ensures compliance for each mode. Especially when the device acts as a master in some working bands and as a client in others; How is compliance guaranteed in each working band?	Only Client mode allowed, all compliance parameters are validated before distribution. Calibration values for each band are stored as H/W in Flash, and the corresponding band is transmitted to TX based on the calibrated value. The default country code is configured as USA upon factory dispatch.
Third party access control	1 Describe whether there is a third party capable of operating a device sold in the United States in a way that would allow the device to operate in violation of the device's authorization if activated in another regulatory domain, frequency, or United States.	Device domain is saved as H/W in Flash as US There is a country code regulatory parameter to limit user to operate the device outside its authorization in the US. End-use cannot access that parameter
	2 If the device allows installation of third-party software or firmware, it describes a mechanism provided by the manufacturer to allow the integration of these features while ensuring that the device's RF parameters cannot be operated outside the range approved for operation in the United States. It includes what controls and/or agreements have been entered into with third-party feature providers to ensure that the device's default RF parameters remain unchanged, and to determine how the manufacturer verifies its functionality.	It is impossible. All the manufactured products do not support any third party firmware upgrade. Cross firmware is not allowed as checksum
	3 For certified transmitter modular devices, the module skin excitation describes how to ensure that the host manufacturer fully complies with these software security requirements for U-NII devices. Describes how to control and manage the driver so that when the module is controlled through driver software loaded on the host, the modular transmitter RF parameters are not modified outside of authorization. 7	The RF parameters of the transmitter module are controlled and managed, and cannot be altered externally except via authorized system software updates. It operates based on hardware calibration values.

Software configuration description		
User configuration guide	1 Describes the user configuration allowed through the UI. If different levels of access are allowed for professional installers, system integrators or end users, please explain the difference.	UI only supports firmware download, wireless scan, and access functions
	a) What parameters can other parties see and configure?	All default parameters are programmed in OTA or in both driver and firmware which would be embedded in system firmware. The professional installer/end-user cannot access the memory. End-use only could wireless scan, access functions.
	b) parameters accessible or correctable by experts Installer or system integrator?	There is not any wifi parameter which is accessible or modifiable to the professional installer.

	(1) The parameters are limited in some way and the installer Are you not entering parameters that exceed the approved parameters?	Yes. Some parameters are programmed in H/W and wifi driver and firmware are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash , memory. The Professional installer/end-user cannot access the flash memory
	(2) What controls are users unable to operate the device from outside? Approval in the US?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S.
	c) What parameters can the end user access or modify?	- End use only could select which AP to connect.
	(1) Are the parameters restricted in some way so that the user or installer does not enter parameters that exceed the approved parameters?	Yes. Some parameters are programmed in H/W and wifi driver and firmware are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash , memory. The Professional installer/end-user cannot access the flash memory
	(2) What controls prevent users from operating their device without permission in the US?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in the US. End-use cannot access that parameter
	d) Is the country code factory set? Can I change it in the UI?	No, the country code cannot be changed in UI.
	(1) If you can change the device Can it be operated only if approved in the United States?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in the US. End-use cannot access that parameter
	e) What are the default parameters when restarting the device?	All default parameters are programmed in H/W or in both driver and firmware which would be embedded in system firmware. The system firmware is programmed and protected in flash memory.
	2 Can the radio be configured in bridge or mesh mode? If so, you may need proof. Additional information is available in KDB. Publication 905462 D02.	Not supported
	3 For devices that can be configured as master and client (including active or passive discovery), if user configurable, describe the controls that exist within the UI to ensure compliance for each mode. If a device acts as a master in some bands and a client in other bands, how is it configured to ensure compliance?	- No. End use cannot configure the wifi device to be as a master or client.
	4 For devices that can be configured with different types of access points, such as point-to-point or point-to-multipoint, and that can use different types of antennas, the presence of an appropriate antenna must be observed to comply with applicable restrictions. Describe the control. Used for each mode Operation. (See Section 15.407(a))	This product is not an access point.