Glassboard, LLC
1060 N Capitol Ave
Suite E-120
Indianapolis, IN 46204

May 20, 2020
Federal Communications Commission
7435 Oakland Mills Road
Columbia, MD 21046

Subject: UNII Software Security Description

Descriptions based on requirements from FCC KDB 594280 D02 v01r03 (2015)

FCC Requirement	Manufacturer Description
General Description	
Describe how any software/firmware updates for elements that can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through the manufacturer's website or device's management system, describe the different levels of security as appropriate.	All software updates shall take place over a TLS secure connection which has a unique public private keypair associated with each device. All firmware updates shall be initiated by the product manufacturer. A unique server token and HTTPS with root CA validation is also used to validate the connection and firmware download request to ensure updates are coming from an authorized server.
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?	The RF parameters are governed by the firmware provided by the RF module manufacturer and to a more limited extent a configuration file stored on the file system of the end device. No modifications to the RF configuration file will be permitted by the end user and shall not be altered by the manufacturer without conducting the required retesting to ensure compliance.
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.	All firmware shall be acquired over a TLS secure connection using HTTPS with root CA validation. The firmware artifact also has embedded checksums to ensure the device firmware download has not been altered or corrupted.
Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The transport of the firmware takes place over an encrypted TLS secure connection that can only be initiated from an authorized

Glassboard, LLC
1060 N Capitol Ave
Suite E-120
Indianapolis, IN 46204

	manufacturer's server.
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?	There is a country code regulatory parameter to limit the end product to operate the device under its authorization in the U.S. This regulatory parameter would define which channel would be available to operate in active or passive scan to meet UNII requirements.
Third Party Access Controls	
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 party has or shall be granted access to alter the radio parameters.
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 end use cases shall not permit third party software or firmware updates to the device. All software and firmware shall come from the original manufacturer.
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	All implementations of our module design shall be directly deployed or overseen by Glassboard. We shall uphold and ensure compliance with the software security requirements for U-NII devices.

Glassboard, LLC
1060 N Capitol Ave
Suite E-120
Indianapolis, IN 46204

Glassboard

RF parameters are not modified outside the grant of authorization.	
Software Configuration Details	
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	There is not any UI to access the Wi-Fi controls or settings outside the SSID and passphrase.
What parameters are viewable and configurable by different parties?	No parameters are configurable by a third party. Wi-Fi connection status, RSSI, connected SSID, and other connection status related parameters may be viewable by the end customer.
What parameters are accessible or modifiable by the professional installer or system integrators (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No parameters are configurable by a professional installer or system integrator. There is a country code regulatory parameter to limit the product's operation outside its authorization in the U.S.
What parameters are accessible or modifiable by the end-user? (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 U.S.?	No parameters are configurable by the end-user. There is a country code regulatory parameter to limit the product's operation outside its authorization in the U.S.
Is the country code factory set? Can it be	The country code is factory set and may only be changed subsequently by a firmware or

Glassboard, LLC
1060 N Capitol Ave
Suite E-120
Indianapolis, IN 46204

changed in the UI? If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	software update if the end device is resold or moved to a new country where modification of the country code would be required to meet their regulatory compliance standards. All devices sold and updated in the US shall have the proper US country code set.
What are the default parameters when the device is restarted?	At device bootup, the wireless driver loads the authorized firmware and RF configuration parameters. This file contains the same RF parameters used in regulatory testing as well as the regulatory country code (US).
Can the radio be configured in bridge or mesh mode? NOTE: If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.	The end device does not support these features.
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?	The end user cannot configure the end device to act as a master or client. Only the end device firmware to support a specific application feature or role has the ability to set the device as a master or client.
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 end device does not support these features.

Glassboard, LLC
1060 N Capitol Ave
Suite E-120
Indianapolis, IN 46204

To the best of my knowledge, the information provided above is true and correct.

Sincerely,

Andrew M Westrick

Andrew M Westrick
VP of Technology
Glassboard, LLC