SOFTWARE SECURITY DESCRIPTION

An applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device; and
2. The device is not easily modified to operate with RF parameters outside of the authorization.

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements. While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards. Also, this guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization. The device complies with KDB 594280D01 and D02

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. Reply: The Wi-Fi settings (maximum power, locale, etc) are built in as pre-defined, hard-coded configurations that are generated at compile time. BLE is not enabled in this product. Firmware updates are uploaded by the the manufacturer (HTTPS and username/password required for upload access) and the device obtains these updates via the server using HTTPS. New firmware images are stored in a secondary location in QSPI flash when they are downloaded to not interfere with the currently loaded image (primary and secondary images). The bootloader will install the new image and keep the previous image as a backup by copying the image from external flash to internal flash. The firmware itself is signed using a private key in a CI pipeline with the public key for verification of the firmware image stored in the bootloader of the device. Authentication failures of the firmware prevent application boot up/execution and the Wi-Fi chip is not powered on.
	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? Reply: The Wi-Fi parameters that are modified in software are: • Disabling DFS channels • Setting the Wi-Fi locale ("US" only) • Maximum TX output power These are elements that are hardcoded in the build configuration and are not modified at runtime.
	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. Reply: New firmware images can only be uploaded by an authenticated user via a username and password. Firmware is downloaded via HTTPS to authenticate the host for the

	firmware. If the host is not authenticated, the download will not proceed. The firmware images are signed with an OpenSSL generated ED25519 private key.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Reply: Firmware images are downloaded via HTTPS using TLS1.2. The encryption mechanism for the download is negotiated by the server. The firmware on the device is authenticated using ED25519, but is not directly encrypted.
	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 eachmode? In particular if the device acts as master in some band of operationand client in another; how is compliance ensured in each band of operation? Reply: Configuration settings are hardcoded as part of the build configuration to limit the TX power for each band. The operating locale is set to "US" in the configuration.
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-solddevice on any other regulatory domain, frequencies, or in any manner thatmay allow the device to operate in violation of the device's authorization ifactivated in the U.S. Reply: No. The device is currently hard coded to only support the US locale and modification of Wi-Fi parameters is not available or exposed on the device.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permitintegration of such functions while ensuring that the RF parameters of thedevice cannot be operated outside its authorization for operation in theU.S. In the description include what controls and/or agreements are inplace with providers of third-party functionality to ensure the devices'underlying RF parameters are unchanged and how the manufacturer verifies the functionality. Reply: Third party software cannot be loaded onto the device.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.

	Reply: The software drivers are part of a single, compiled image. There is not a separate, external or runtime driver that can be loaded. The Wi-Fi module parameters are set only at compile time and are not modified or available for modification at runtime.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE	
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. Reply: For Wi-Fi related settings, a user can only update or modify the access point to use when operating in station mode. This is modified through the TagoRun phone application which is utilized by an end user during initial setup or an authorized installer.
	a) What parameters are viewable and configurable by different parties? Reply: For Wi-Fi related settings, only the Wi-Fi access point name is viewable by an authorized user or professional installer
	b) What parameters are accessible or modifiable tothe professional installer? Reply: For Wi-Fi related settings, only the Wi-Fi access point name is viewable by an authorized user or professional installer
	i. Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply: Wi-Fi parameters are hardcoded to not exceed authorized limits and cannot be changed at runtime
	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? Reply: Only authenticated firmware can run. Authorized parameters are hard coded in firmware and are not updated at runtime (nor do any inputs exist for an end user to modify them).
	c) What parameters are accessible or modifiable by the end-user? Reply: For Wi-Fi related settings, only the Wi-Fi access point name is viewable by an authorized user or professional installer

	i. Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply: The only available parameter to modify does not impact authorized limits.
	ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? Reply: Only authenticated firmware can run. Authorized parameters are hard coded in firmware and are not updated at runtime (nor do any inputs exist for an end user to modify them).
	d) Is the country code factory set? Can it be changedin the UI? Reply: The country code is set to US in the firmware build and cannot be changed
	i. If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Reply: N/A
	e) What are the default parameters when the deviceis restarted? Reply: • US country code • 2.4GHz Wi-Fi bands limited to maximum +15dBm • 5GHz channels 36 – 64 limited to maximum +9dBm • 5GHz channels 100 – 132 limited to maximum +11 dBm • 5GHz channels 136 – 177 limited to maximum +13 dBm
	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. Reply: No
	3. For a device that can be configured as a master andclient (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? Reply: The device is only used in AP mode for provisioning and set up (configure target access point in station mode). This is enabled via a button press of more than 15 seconds while the device is operational. No radio parameters are configurable in either of these modes as the limits are hardcoded into the firmware and are unavailable for modification at runtime.

	4. For a device that can be configured as different typesof 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)) Reply: Onboard antenna and only one access point mode are available to use.