IoT Defense Inc.

Federal Communications Commission
Authorization and Evaluation Division
7435 Oakland Mills Rd.
Columbia, MD

Date: 2018-11-23
FCC ID: 2AP2U-SN3E

U-NII Device Security Statement

To Whom It May Concern

SOFTWARE SECURITY DESCRIPTION	
General Description	
1.Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer’s website or device’s management system, must describe the different levels of security.	Re: Only system software, it can be update by “system upgrade” software. The level of security is middle.
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?	Re: For wireless, the manufacturers of wireless have inherent firmware which will not be modified by the whole machine firmware or software RF parameters.
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.	Re: The wireless is in accordance with WIFI 802.11 protocol. The RF parameters are in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software.
4.Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Re: wpa-psk TIKP, wps-psk AES, wep40, wep104
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	Re: It is not working in DFS bands, and compliance for related FCC rules.

device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?	
Third-Party Access Control	
1. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root
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.	Re: The wireless is in accordance with WIFI 802.11 and protocol. The RF parameters are in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software. Before installation of software and firmware, the system will check the certificate and signature, and only legal circumstances permit the 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.7	Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.

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	Re: end user
a) What parameters are viewable and configurable by different parties?	Re: NONE
b) What parameters are accessible or	Re: NONE

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?	Re: YES
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Re: The firmware is write in ROM. The end user cannot modify it.
c) What parameters are accessible or modifiable to by the end-user?	Re: NONE
d) Is the country code factory set? Can it be changed in the UI?	Re: The country code is fixed for US, and it cannot be changed in the UI.
e) What are the default parameters when the device is restarted?	Re: All the parameters is fixed for US, whatever the device is restarted or not.
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.	Re: No
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?	Re: No
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))	Re:No

Sincerely,
Company: IoT Defense Inc.

Signature

Tilaraj Roychoudhury

……………………………………

Typed name and Title: Tilakraj Roychoudhury /CEO