Teradek, LLC
34B Mauchly Irvine, CA 92618 United States

FCC ID: 2AFNQ-WUBM273ACN

Software Security Description – KDB 594280 D02v01r01 Section II		
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.	The User can download the firmware from PLANET website manually.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	Wi-Fi radio frequency parameters can be changed via UI without any hardware changes; The regulatory domain frequencies was limited by the country code, all were verified by HW RF validation and stored in device embedded FLASH memory
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.	No, but has a signature verification and checksum in the firmware header to ensure the firmware is legitimate.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	A signature verification and checksum in the firmware header to ensure the firmware is legitimate.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	No encryption methods were applied in the firmware
	6. 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 device can be configured as a client. Chipset vendor ensures its can compliance for 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.	A signature verification and checksum in the firmware header to ensure the US version of firmware.
	2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.	1) A signature verification and checksum in the firmware header to ensure the US version of firmware. 2) Regarding the GPL release, will provide the UI's binary code instead of source code.
	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.	All critical radio parameters including maximum output power, frequency bands of operation, modulation types, passive/active scanning controls are programmed into the EEPROM and will not be accessible or changed by third parties.

Teradek, LLC
34B Mauchly Irvine, CA 92618 United States

Your Sincerely,

Name/Title: Marius K van der Watt / V.P Engineering
Company name: Teradek, LLC
ADD: 34B Mauchly Irvine, CA 92618 United States
TEL: (888) 941-2111 110
E-mail: marius.vanderwatt@teradek.com
Date: 2016/2/1