GoPro, Inc.
3025 Clearview Way, San Mateo, CA 94402, USA

Federal Communications Commission 30/03/2022
Oakland Mills Road
Columbia MD 21046
Model： STMD1
FCC ID: CNFSTMD1
Subject: Software security requirements for U-NII device.
The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03.

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.	Any software/firmware updates can not affect RF parameters.
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?	The RF parameters/limits are stored in a separate part of the non-volatile storage and not updated or changed with the firmware updates.
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.	There are currently no authentication protocols in place to check for a valid firmware outside of product registration and serial number.
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	Firmware are not encrypted. RF related parameters/limits are stored in a sperate part of non-volatile storage and are not part of the firmware.
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 device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?	The device is client device without radar detection function
3rd Party Access Control	
1. 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.	Third parties do not have the capability to change radio parameters or country domains.

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.	This device does not permit third-party software or firmware installation and only the permitted person can update the software or firmware via special command.
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.	None parameters are viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings.
SOFTWARE CONFIGURATION DESCRIPTION	
1. To whom is the UI accessible? (Professional installer, end user, other.)	
a) What parameters are viewable to the professional installer/end-user?	This device is not subject to professional installation.
b) What parameters are accessible or modifiable to the professional installer?	N/A-This device is not subject to professional installation.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	N/A-This device is not subject to professional installation.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	N/A-This device is not subject to professional installation.
c) What configuration options are available to the end-user?	
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	RF parameter are programmed in flash memory and not accessible to the end-user.

GoPro, Inc.
3025 Clearview Way, San Mateo, CA 94402, USA

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	RF parameter are programmed in flash memory and not accessible to the end-user. This includes the country code regulatory parameters.
d) Is the country code factory set? Can it be changed in the UI?	
i) If so, what controls exist to ensure that the device can only operatewithin its authorization in the U.S.?	The country code is factory set and can not be changed in the UI.
e) What are the default parameters when the device is restarted?	At each start up the factory configured country code and antenna gain are read from non-volatile memory.
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.	Not supported.
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?	The device is client device without radar detection function.

Best Regards

Name: Michelle Tsai

Title: Director of Product Safety and Compliance
Company: GoPro, Inc
Address: 3025 Clearview Way, San Mateo, CA 94402, USA
E-mail: michelletsai@gopro.com