GoPro, Inc.
3000 Clearview Way, San Mateo, CA 94402, USA

SOFTWARE SECURITY DECLARATION FOR U-NII DEVICES
Product: Camera, FCC ID: CNFSPCC1, KDB 594280 D02 U-NII Device Security v01r03

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.	The firmware updates are published through the GoPro site. Updates can also be done through the GoPro IOS and Android APPs. Product registration with serial number is required before FW updates are downloaded.
	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?	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 RF-related software/firmware is valid. Describe in detail how the RF-related 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 any encryption methods used to support the use of legitimate RF-related software/firmware.	n/a
	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?	This device is only a client in 5 GHz operation and does not operate as master.

Third-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 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.	N/A – Transmitter Is integrated into the device and is not a module.
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,	The UI is accessible to anyone using the device.
	a) What parameters are viewable and configurable by different parties?	User can select the working band of the WIFI module: 2.4G or 5GHz.

	b) What parameters are accessible or modifiable to the professional installer or system integrators?	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
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	N/A

USER CONFIGURATION GUIDE (cont.)	c) What parameters are accessible or modifiable by the end-user?		User can select the working band of the WIFI module: 2.4G or 5GHz.
		i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The built in regulatory settings cannot be changed by the end-user.
		ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	There are no restrictions on operating the device outside of US.
	d) Is the country code factory set? Can it be changed in the UI?		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?		NA – Device is only a client in 5 GHz operation
	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))		NA – Device is only a client in 5 GHz operation