

SONY

Sony Corporation
1-7-1 Konan Minato-Ku Tokyo, 108-0075 Japan

Date: August 1st, 2017
FCC ID: AK8LFS50G

Software Security Description

We, **Sony Corporation**, hereby declare that requirements of **LF-S50G** have been met and shown on the following question.

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. Description: User only use Auto Magic website update firmware.
	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? Description: The Wi-Fi channel is limited by the country code.
	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. Description: The firmware disable all debug method, example, ADB, SSH and so on.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. Description: Using AES checking the firmware before it been installed.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware. Description: Using AES, 3DES
	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? Description: In setup mode, the device as the master can be found on the phone. If setup success, it become the client connect to the AP.
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. Description: No.

SONY

Sony Corporation
1-7-1 Konan Minato-Ku Tokyo, 108-0075 Japan

	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. Description: The devices will check the firmware hardware version and software version before the firmware been installed on the devices.
	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. Description: Encryption mechanism.

Software Security Description	
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.) Description: End user.
	a) What parameters are viewable to the professional installer/end-user? Description: Volume / dimmer level / language / location
	b) What parameters are accessible or modifiable by the professional installer? Description: none
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: none
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: the user cannot use the web service without its authorization.
	c) What parameters are accessible or modifiable to by the end-user? Description: volume / location / language / dimmer level
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: Parameters is limited, and installers will not enter parameters that exceed those authorized.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: the user cannot using the web service without its authorization.

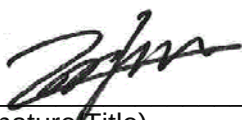
SONY

Sony Corporation
1-7-1 Konan Minato-Ku Tokyo, 108-0075 Japan

	d) Is the country code factory set? Can it be changed in the UI? Description: Factory set cannot change the country code. It can't be change in the UI.
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Description: Using country code control the Wi-Fi channel.
	e) What are the default parameters when the device is restarted? Description: The parameters will save before it reboot.
	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. Description: It cannot support bridge / mesh mode.
	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? Description: In setup mode, the device as the master can be found on the phone. If setup success, it become the client connect to the AP.
	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)) Description: The devices have only one antenna. Using TDM technology.

If any questions regarding this declaration, please don't hesitate to contact us.

Sincerely



(Signature/Title)
Takeshi Kobayashi
Product Safety Manager
Product Compliance Section
Quality Assurance Department
Sony Video & Sound Products Inc.