SOFTWARE SECURITY DESCRIPTION		
No	General Description	LG description
1	Describe how any software/firmware update will be obtained, downloaded, and installed.	The software/firmware update is bundled, as part of the LGE Android software update, and the user or installer cannot modify the content. The installation and/or update proceeds automatically once the user accepts to install/update the software/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?	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release is verified by the Grantee before release. And there is no special authentication algorithm to protect this file. But normal user can't modify this file because it needs root permission.
3	Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	Yes, software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.
4	Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	- Q fusing : Only LGE's authorized member can build and release SW that can be updated to device. - SE Linux function : It provide enhanced security policy to kernel. So modification and wrong access by third party application is prohibited.
5	Describe, if any, encryption methods used.	Yes, encryption using proprietary internal software.
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?	Country code is used to decide passive scan or active scan. And the country code is obtained by conneced mobile network's MCC value. If device can't get country code the device use default value(default value means minimum set of reguration domain of all country).
No	Third-Party Access Control	LG description
1	How are unauthorized software/firmware changes prevented?	Already mentioned Q fusing and SE linux can provide sufficient security function.
9	Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	There are no way to load modifed driver because it needs root permission. And user can't get root permission.

10	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.	No, refer to the answer above.
11	What prevents third parties from loading non-US versions of the software/firmware on the device?	SW download tool ensure that non-US version is not loaded on US device.
12	For modular devices, describe how authentication is achieved when used with different hosts.	We don't make module.

SOFTWARE CONFIGURATION DESCRIPTION		
No	USER CONFIGURATION GUIDE	LG description
1	To whom is the UI accessible? (Professional installer, end user, other.) a) What parameters are viewable to the professional installer/end-user? b) What parameters are accessible or modifiable to the professional installer? i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? 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? ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? 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 operate within its authorization in the U.S.? e) What are the default parameters when the device is restarted?	a) Link Rate and Signal Strength, WiFi Security method and channel information. b) Nothing c) Nothing d) Yes, No e) Nothing is changed. We always use certified setting.
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.	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?	Only WiFi Hotspot can change WiFi channel that is allowed.
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))	We don’t' use different type of antennas.