SOFTWARE SECURITY DESCRIPTION (FCC ID : ZNFX540HM)

No	General Description	LG 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 software/firmware update is bundled, as part of LGE 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. User can obtain the LGE software update via LGE website or FOTA.
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?	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release is verified by Grantee before release. If required, Grantee will follow FCC permissive change procedure.
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.	Software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols. The device inoperable if signed value is invalid through modification.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Encryption using proprietary internal software.
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 country code which is obtained from mobile network's MCC value is used to ensure full compliance with band operation. If the device can't get the country code, it uses default value which is the minimum set of reguration domain of USA.
No	**Third-Party Access Control**	**LG description**
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.	Only Grantee can release or make changes to the software/firmware using proprietary secure protocols. Any third parties can't operate on domain, frequencies.
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.	LGE device supports strong security implementation. Grantee proprietary hardware platform, software tools and proprietary protocols are required to replace a new firmware. Even if some 3rd party applications replace the firmware in violation of security, it's inoperable with the device.
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.	Not applicable, this device is not a module.

SOFTWARE CONFIGURATION DESCRIPTION

No	USER Configuration Guide	LG description
1	Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. a. What parameters are viewable and configurable by different parties? b. What parameters are accessible or modifiable by the professional installer or system integrators? (1) Are the parameters in some way limited, so that the 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.? c. What parameters are accessible or modifiable by the end-user? (1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? (2) What controls exist so 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? (1) If it can be changed, 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?	All users have access to Link Rate and Signal Strength, Wi-Fi Security method and channel information. Any other parameters except for parameters(Link Rate and Signal Strength, Wi-Fi Security method and channel information) are not accessible and all parameters are not modifiable. a. Link Rate and Signal Strength, WiFi Security method and channel information. b. 1) & 2) Nothing is accessible or modificable by 3rd party or Installers. c. 1) Yes, it's encripted and nobody can access it except for the manufacturer. 2) Nothing exists. d. Yes, it's set-up but it's never can be changed in the UI. e. Nothing is changed. It's always set-up based on the regulatory domains.
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 defferent type of antennas.