Software Security Description

Applicant describe the overall security measures implemented in the device that ensure that the device cannot be modified by any RF-related software changes by third parties to operate outside the authorized RF parameters without further approval from the FCC

The description of the RF-related software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the RF-security requirements.

SOFTWARE SECURITY DESCRIPTION	
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. There is a 4-PIN service port based on USB interface. Any new software/firmware can be obtained from the qualified database inside HIKVISION.
	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? There are no any interfaces inside the software/firmware to modify the radio frequency parameters.
	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 is a qualified database for software revision control inside HIKVISION. Any software/firmware modification will be under QMS process control.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Any software/firmware modification will have the verification procedure and verification results and release letter and impact analysis report based on QMS/SDLC process. Any modification will be highlighted on the release letter, and the impact analysis will also have a review. Verification procedure and verification results will be performed based on the release letter and impact analysis report.
	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 that can be configured as a client with passive scanning
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. No, the device not permits operates in violation of the device's authorization.
	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. No, the device not permits third-party software or firmware installation.
	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. The device is not a Certified Transmitter modular devices

SOFTWARE CONFIGURATION DESCRIPTION	
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, describe the differences.
	a What parameters are viewable and configurable by different parties? No any 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? The device not permits operates in violation of the device's authorization.
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Any modification will be highlighted on the release letter, and the impact analysis will also have a review. Verification procedure and verification results will be performed based on the release letter and impact analysis report.
	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? There are no any interfaces is the UI accessible.
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? There are no any interfaces inside the software/firmware to modify the radio frequency parameters.
	d Is the country code factory set? Can it be changed in the UI? The country code factory is set? It can't 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? When the device is restarted, the default parameters restore to the original authorization.
	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? The device can be only as the client with passive scanning
	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)) The device can't be configured as access points. Only Mobile and Portable Client device mode. The antenna is PIFA antenna and no consideration of replacement.