F@st 5260CV	
SOFTWARE SECURITY DESCRIPTION	
General Description	Sagemcom response
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.	A new software update is initiated through the ACS (Automatic Configuration System), which instruct the software to retrieve a new software image from a given URL. ACS is protected by login and passwrod.
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?	We set the default parameters we get in the BSP/WiFi driver in OpenRG rg_conf We have only authorized 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.	Per TR-69 specifications, the software initiates a connection to the ACS (ACS cannot connect to the software), based on factory settings . Only the ACS can instruct the software to download a new image and provides the URL. This is a workflow that personal initiate and the ACS is within secured network. The Downloaded firmware is signed with an RSA key which is validated by OpenRG before upgrading
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The image is not encrypted only signed.
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?	Not relevant, the device is only 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.	Only the ACS can manage the device. All other management interfaces are disabled
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.	In general, the end user has no access to the flash memory and thus cannot burn a new image on top of the existing one. A new image is only updated per the above described procedure. On top of the above, the image itself on the flash is compressed and thus changes must be done on the entire opened image and re-compressed again in order to successfuly be loaded after reboot. There is also a checksum of the compressed image that is being verified in order to ensure the image was not corrupted (by user or defective memory).
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 drivers are part of the entire image containing all software components. There is no telnet or CLI access to a manfucature device, thus a 3rd party have no access to replace a driver at run-time. 3rd parties cannot replace the software on the device, per the answers in "General Description" section. As such, the the modular transmitter RF parameters cannot be are not modified outside the grant of authorization.

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.	The UI is accessible to the end user and professional installer. In addition, a support call personnal can also access the UI when in need.
a. What parameters are viewable and configurable by different parties?	The user\installer can set the SSID and Channel Only.
b. What parameters are accessible or modifiable by the professional installer or system integrators?	Same as end user
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes, the UI has input verification that ensures only valid values are entered.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user UI has limitation on the values the user can enter and verification is done on those parameters. The UI itself is located in core network, and changes are then moved through APIs to the ACS, which has value verification per the data model. In addition the driver country code is us and it will not allow invalid settings - need to verify with vendor.
c. What parameters are accessible or modifiable by the end-user?	Wifi related: SSID, Channel
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes, the UI has input verification that ensures only valid values are entered.
(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	The end user UI has limitation on the values the user can enter and verification is done on those parameters. The UI itself is located in core network, and changes are then moved through APIs to the ACS, which has value verification per the data model.
d. Is the country code factory set? Can it be changed in the UI?	The country code is factory set and it cannot be changed via 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?	If the device is restarted all the parameters have their default values from radio calibration done in factory and conform to FCC.
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.	There is no such option in the UI to do so.
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?	Not relevant, the device is only master.
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))	Not applicable. It cannot be configured differently through OpenRG UI