Samsung Electronics Co.,LTD.
129, Samsung-ro,Yeongtong-gu
Suwon-City, Gyeonggi-do, 443-742 Korea

Date: March 6. 2015

Subject: U-NII device Security
FCC ID: A3LSMP355M

To Whom it MayConcern

We attest the following regarding KDB 594280 D02 U-NII device Security.

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Security.

The information below describes how we maintain the overall security measures and systems so that only:

1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

General Description	
1. Describe how any software /firmware update will be obtained, downloaded, and installed.	Software/Firmware is pushed from the Samsung's authorized servers by means of encryption by OTA or PC tool via USB. But update packages are encrypted and digitally signed by proprietary key.Therefore, user cannot obtain unauthorized 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 frequency parameters are embedded at the time of production in the factory per FCC approved. These parameters are therefore fixed at the factory such that they will not exceed the authorized values.
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 are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.Secure Sockets Layer is used as a protocol for encrypting information over the internet. Therefore, Samsung ensure that the source of the software/firmware is legitimate.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details	Software/Firmware release is pushed from the Samsung's authorized servers by means of proprietary encryption. And, update packages are encrypted and digitally signed. Secure Socket Layer is used as a protocol for encrypting information over the internet.
5. Describe, if any,encryption methods used?	Yes, by means of proprietary public key encryption.

General Description	
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?	The device will be able as master only ISM band and UNII 1 and 3 bands. For DFS bands, device can not be master device with DFS detection. For compliance, device will transmit under approved power. And user can't access to change Master/client feature per band.

3rd Party Access Control	
1. How is any unauthorized software/firmware change prevented?	Samsung releases the firmware/software directly from Samsung's servers through proprietary encryption protocol. Samsung can ensure its server because the signature of downloaded binary is checked before updating software/firmware.
2. 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.	No. As mentioned above, RF parameters or other parameters which impact device compliance are fixed at time of production in the factory.
3. 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, third parties don't have capability to access and change radio parameters.
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Samsung proprietary hardware platform and software tool chain including boot-loader are not available to 3rd parties.
5. For modular devices, describe how authentication is achieved when used with different hosts.	Not a modular device

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
1. To whom is the UI accessible? (Professional installer, end user, other.)	The UI is accessible to anyone using the device. But the UI never gives access for specific operation parameters which are frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings.
a) What parameters are viewable to the professional installer/end-user?[2]	Nothing to control the radio operation parameter for professional installer/end-user
b) What parameters are accessible or modifiable to the professional installer?	This device is not subject to professional installation

[1] This section is required for devices which have a "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter. Supporting information is required in the operational description. The operational description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

[2] The specific parameters of interest for this purpose are those that may impact the compliance of the device. These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
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?	The end user has no access to configuration settings that could change the radio operation parameters.
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?	The country code is factory set and it is never changed by 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?	The specific operation parameters which are frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings are never changed after even being restarted.
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.	This device cannot be configured in a bridge or 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?	The device will be able as master only ISM band and UNII 1 and 3 bands. For DFS bands, device can not be master device with DFS detection. For compliance, device will transmit under approved power. And user can't access to change Master/client feature per band.
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 will be able as master only ISM band and UNII 1 and 3 bands. For DFS bands, device can not be master device with DFS detection. For compliance, device will transmit under approved power. And user can't access to change Master/client feature per band. The device only contains integrated antennas that are not user selectable or interchangeable .