HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

Federal Communication Commission
7435 Oakland Mills Road
Columbia, MD 21046
August 4, 2016

RE: KDB 594280 D02 U-NII device Security v01r03
FCC ID: APIMLNO519

Software Security Requirements for U-NII devices

To Whom It May Concern:

Harman International Industries, Inc. declares that No519 meets all security requirements listed below as required in FCC Part 15 Subpart E Rules required for Unlicensed – National Information Infrastructure (U-NII) equipment.

Software Security Description

General 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 update is done via HTTP Internet Update from a Harman maintained Website. There is also the option to do an "emergency upgrade" via USB. The update file is a compiled binary, not readable, and no parameters can be changed after the file has been created from the build process. When updating, the bootloader verifies the checksum of the binary and only installs it if it is a valid build. The file is not encrypted nor signed.

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?

RF Parameters are determined by the binary image. The end user cannot modify RF 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.

The No519 looks for a specific Hard Coded URL (firmware.MarkLevinson.COM) and filename (sfupdate) to find the Harman Server and the update file. The update file is verified by checksum.

4) Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

The user do not have any access to the legitimate RF-related software/firmware.

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 No519 operates as client only in the 5GHz range.

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 third parties have the capability to operate this device on any 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 United States.

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

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.

The device does not permit third-party software or software 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 drivers are controlled by the developers and integrated into the firmware binary file and there is no ability for the end user to access or modify them.

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.

None of the mentioned parameters are viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1a) What parameters are viewable and configurable by different parties?

No such parameters are accessible or modifiable by any parties.

1b) What parameters are accessible or modifiable by the professional installer or system integrators?

No such parameters are accessible or modifiable by professional installers or system integrators.

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

1b1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1b2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1c) What parameters are accessible or modifiable by the end-user?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1c1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1c2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1d) Is the country code factory set? Can it be changed in the UI?

The No519 has no country code, thus it cannot be changed.

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

1d1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).

1e) What are the default parameters when the device is restarted?

When the device is restarted, the previously used settings are loaded.

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.

The radio cannot be operated in 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?

Client mode (normal operation) operates in both the 2.4GHz and 5GHz bands using passive scanning. Master Mode operates only in the 2.4GHz band. Compliance is ensured because the WiFi driver and all RF parameters are not adjustable by the user.

The Access Point mode (Soft-AP mode) is for WiFi setup only. In this mode, the end user can connect to the No519 as if he would connect to an Access Point (via a computer or mobile device). Once connected the end user can scan e.g. for his default home WiFi network and configure the No519 so it can join this network. After the configuration, the Access Point mode will be switched off again.

This Access Point mode is just another method to link the No519 into the users personal home network. Alternatively, this can also done via the Local UI menu or via a Network cable, connected to the RJ45 port of the No519.

The end-user has no access to RF parameters (Frequency Channel, Channel Bandwidth, Channel Power or other Countries parameters).

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

These are the accessible parameters to end-user during Soft-AP mode.

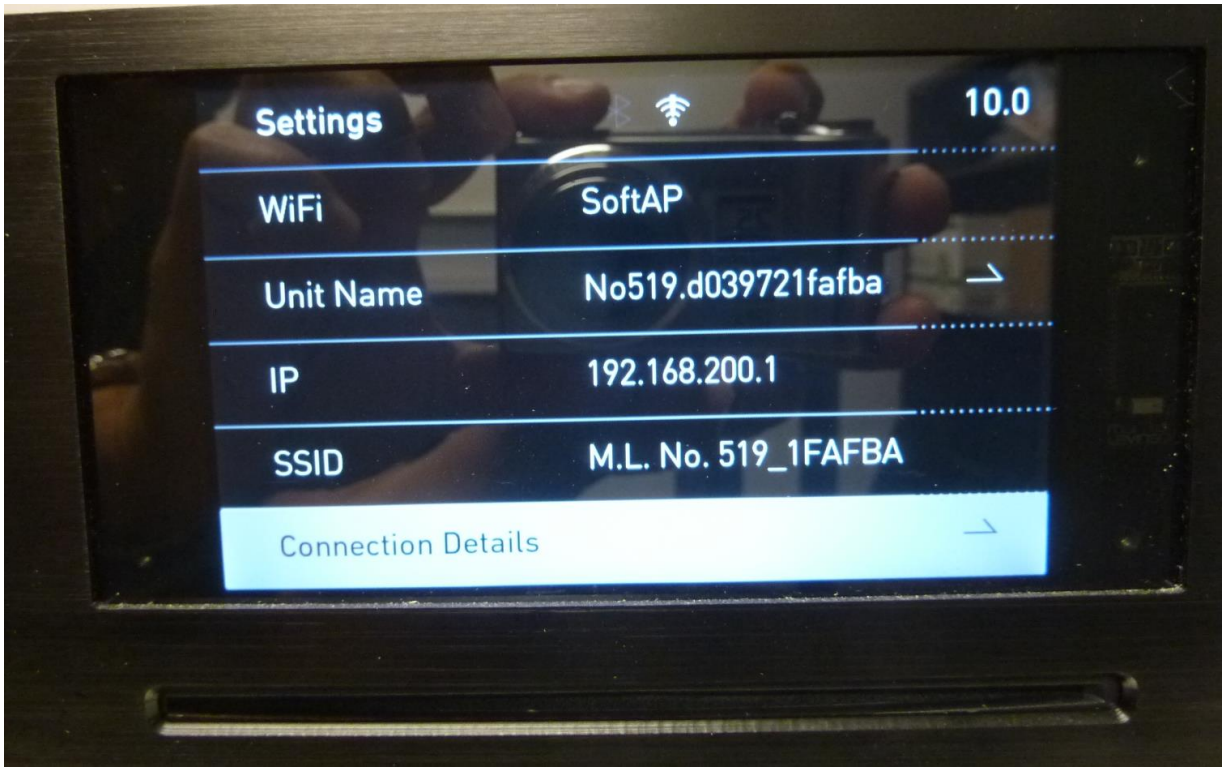

Figure 1

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

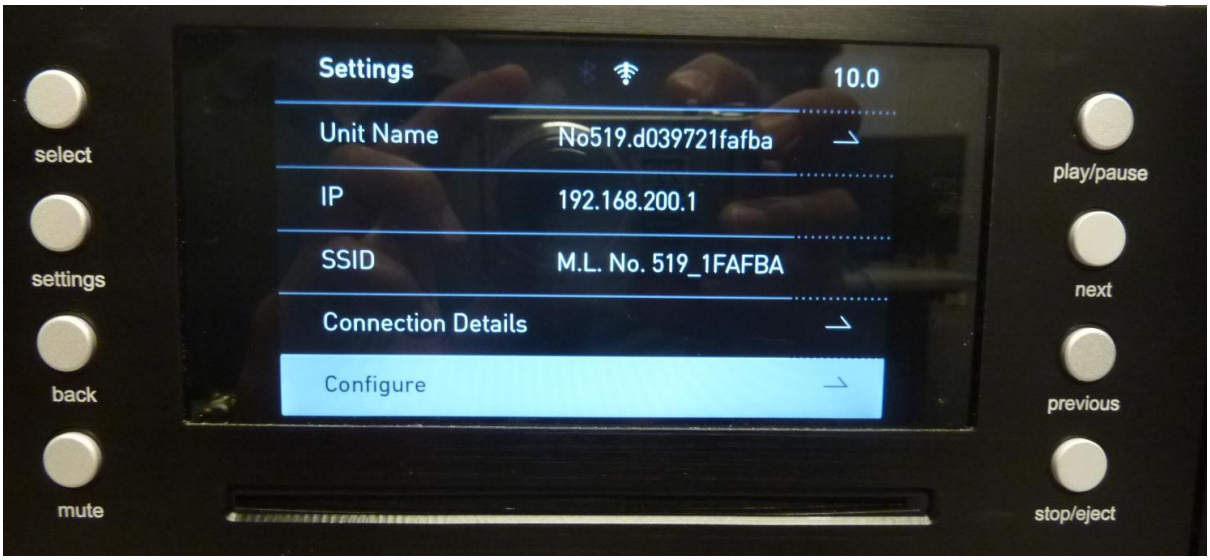

Figure 2

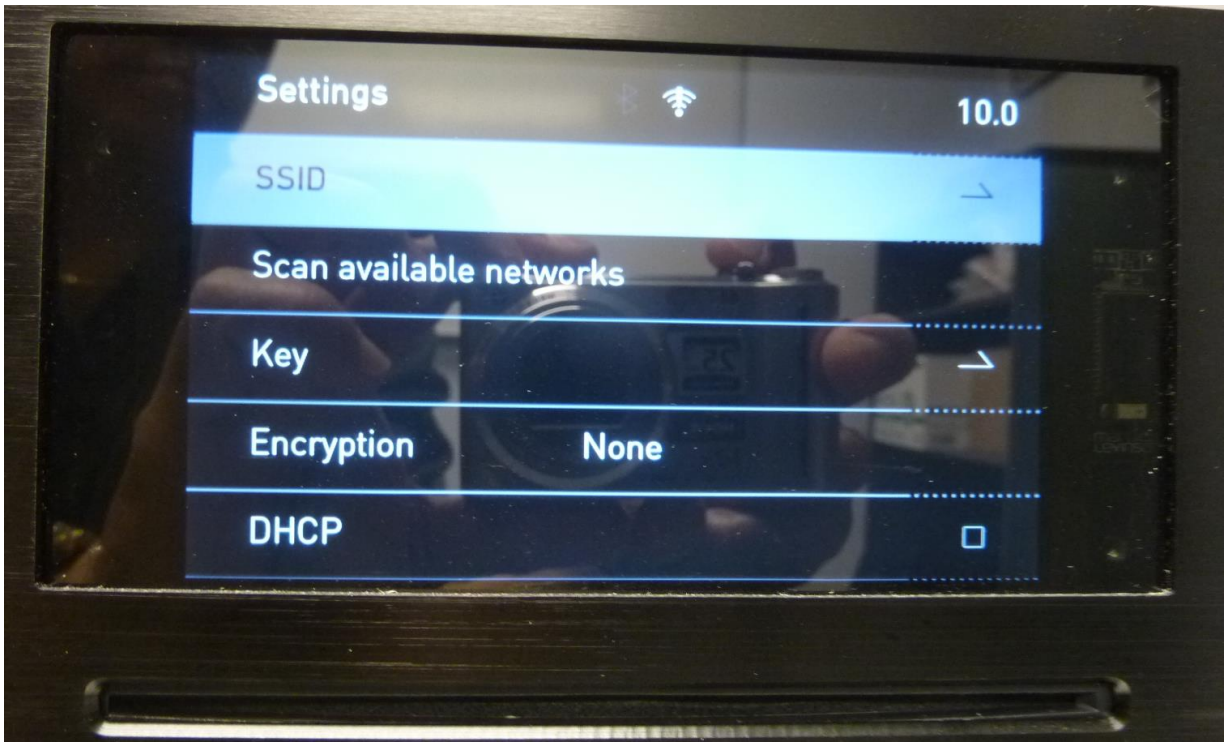

Figure 3

HARMAN International Industries, Inc.
8500 Balboa Blvd.,
Northridge, CA 91329

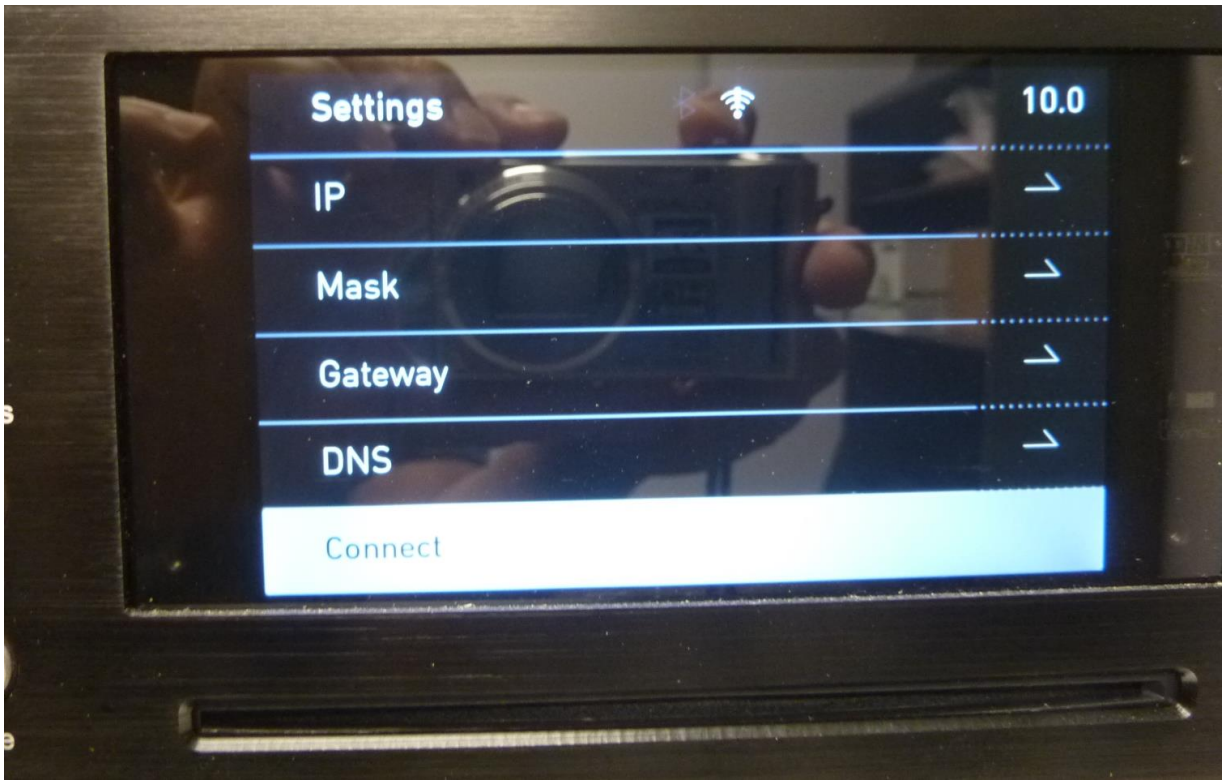

Figure 4

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))

Different types of access points, such as point-to-point or point-to-multipoint, and use of different types of antennas is not supported in the No519.