Software Security Requirements For U-NII Devices

I. General Description

(1) Describe how any software/firmware update will be obtained, downloaded, and installed.

Ans:

(a) It will be obtained by the ODM : ☒ Yes ☐ No

(b) It will be downloaded from the ODM website : ☒ Yes ☐ No

(c) It will be installed by the end-user : ☒ Yes ☐ No

(2) Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes.

Ans: When the FCC Part 15E Grant is updated under a C2PC to include U-NII bands 2 & 3, updated firmware will be posted to the online product support site. Existing customers will have the option of installing the new software image to enable operation on U-NII bands 2 & 3. Security measures to prevent unauthorized operation are covered in later questions.

Are these parameters in some way limited, such that, it will not exceed the authorized parameters?

Ans: The firmware has been compiled as binary file. It is not possible to change the RF parameters. It is a read-only format provided by the ODM.

(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.

Ans: ☒ Yes ☐ No

The product includes a product name check and code signing algorithm for the firmware, effectively preventing non-compliant operation for US-based customers.

(4) Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.

Ans: ☐ Yes ☒ No

(5) Describe, if any, encryption methods used?

Ans: ☒ Yes ☐ No

The firmware has been compiled as binary file. It is not possible to change the RF parameters. It is a read-only format provided by the ODM.

(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?

Ans: ☐ Yes ☒ No

This device can not be configured as a master and client.

II. Third-Party Access Control

(1) How are unauthorized software/firmware changes prevented?

Ans: This product includes a separate SKU for the US, Canada and Latin American market. The product sold in the US includes dedicated firmware to comply with the applicable FCC requirements. The end-user can only update the firmware with an image that complies with the FCC rules. This is accomplished by instituting a product name check and code signing for the firmware, effectively preventing non-compliant operation for US-based customers.

(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.

Ans: ☒ Yes ☐ No

The end-user can upgrade the firmware to enable U-NII bands 2 and 3 after the FCC Part 15E Grant is updated to include these bands.

As detailed in the response to question 1, the product sold in the US includes dedicated firmware to comply with the applicable FCC requirements. The end-user can only update the firmware with an image that complies with the FCC rules. This is accomplished by instituting a product name check and code signing for the firmware, effectively preventing non-compliant operation for US-based customers.

(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.

Ans: ☐ Yes ☒ No

As detailed in the response to question1, we have assigned a separate product SKU for customers located in the US, Canada and Latin America. The end-user cannot enable any frequencies, regulatory domains, or operational modes that are not in compliance with the FCC requirements.

(4) What prevents third parties from loading non-US versions of the software/firmware on the device?

Ans: ☒ Yes ☐ No

We ship a dedicated product SKU to US-based customers. The end-user can only update the firmware with an image that complies with the FCC rules. This is accomplished by instituting a product name check and code signing for the firmware, effectively preventing non-compliant operation for US-based customers.

(5) For modular devices, describe how authentication is achieved when used with different hosts.

Ans: HP maintains control of the host products the radio modules will be installed in. Each Host device includes unique software to achieve authentication. This is accomplished by instituting a product name check and code signing for the firmware, effectively preventing non-compliant operation for US-based customers.

User Configuration Guide

(1) To whom is the UI accessible? (Professional installer, end user, other.)

Ans: ☐ Professional installer ☒ End user ☐ Other

(a) What parameters are viewable to the professional installer/end-user?

Ans:

☐ Frequency of operation ☒ Power settings ☒ Country code

☒ Other: Authorized channel, bandwidth, modulation.

(b) What parameters are accessible or modifiable to the professional installer?

Ans: ☒ Authorized frequency of operation ☒ Authorized power settings ☐ Authorized Antenna

☒ Country code

☒ Other: Authorized channel, bandwidth, modulation.

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

Ans: ☒ Yes ☐ No

The Authorized channel, bandwidth, modulation and country code parameters can be modified by the end-user, but regardless of the settings, FCC-compliant operation will be maintained. The country code setting for non-US countries will limit the available channels in some cases, but enablement of non-authorized channels is not possible. The power setting can only reduce the Authorized power setting to 100%, 50%, 25%, 12.5% and min.

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

Ans: We have assigned a separate product SKU for customers located in the US, Canada and Latin America. The end-user cannot enable frequencies, regulatory domains, or operational modes that are not in fulll compliance with the FCC requirements.

(c) What configuration options are available to the end-user?

Ans:

☐ Frequency of operation ☒ Power settings ☒ Country code

☒ Other: Authorized channel, bandwidth, modulation.

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

Ans: ☒ Yes ☐ No

We have assigned a separate product SKU for customers located in the US, Canada and Latin America. The end-user cannot enable frequencies, regulatory domains, or operational modes that are not in fulll compliance with the FCC requirements.

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

Ans: We have assigned a separate product SKU for customers located in the US, Canada and Latin America. The end-user cannot enable frequencies, country domains, or operational modes that are not in fulll compliance with the FCC requirements.

(d) Is the country code factory set?

Ans: ☒ Yes ☐ No

Can it be changed in the UI?

Ans: ☒ Yes ☐ No

i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Ans: We have assigned a separate product SKU for customers located in the US, Canada and Latin America. The end-user cannot enable frequencies, country settings, or operational modes that are not in fulll compliance with the FCC requirements.

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

Ans: Factory setting: US country code

(2) Can the radio be configured in bridge mode?

Ans: ☐ Yes ☒ No

Can the radio be configured in mesh mode?

Ans: ☐ Yes ☒ 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 to ensure compliance.

Ans: ☐ Yes ☒ No

This device can not be configured as a master and client.