Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

November 12, 2015

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

I. INTRODUCTION

On March 31, 2014, the Commission revised the rules in Part 15 that permits U-NII devices in the 5 GHz Band.[1] As part of that revision, the Commission required that all U-NII device software that controls the RF parameters that ensure compliance with the Commission's technical rules for preventing harmful interference must be secured.[2] The purpose of this rule is to prevent modifications to the software that could, for example, disable dynamic frequency selection (technology necessary for preventing interference to radars), enable tuning to unauthorized frequencies, increase power above authorized levels, etc.[3] The rule is not intended to prevent or inhibit modification of any other software or firmware in the device, such as software modifications to improve performance, configure RF networks or improve cybersecurity. These types of software and firmware modifications, including updates to address security vulnerabilities are known to be highly desired by many users and manufacturers are encouraged to design their systems to permit such software upgrades while ensuring security of the portion that controls compliance with the FCC technical requirements.

The Commission decided not to set specific protocols or methods for securing the parts of the software that control compliance with the FCC technical requirements for controlling harmful interference. However, the methods used by manufacturers to implement the RF security requirements must be well documented in the application for equipment authorization. In this document, we provide general guidance on the type of information that should be submitted in the equipment authorization application. The security description provided in the application must cover the RF software security, configuration, and authentication protocols descriptions, as appropriate. This guidance applies to master and client devices. Special circumstances that apply only to client devices are also addressed.[4]

[1] *See Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report and Order*, ET Docket No. 13-49 (2014) (1st R&O).

[2] The term "RF parameters" includes any function that impacts the compliance with our rules. In addition to obvious values like power, frequency, bandwidth, modulation, and emissions mask, it includes any other parameters related to compliance of EMC, SAR, HAC, and similar regulations and, in some cases, usage functions like those specified in Parts 90 and 95. This also includes specifications for MURS, WMTS, MBANS, and even newer services in Part 96.

[3] *See* § 15.407(i)(1). For ensuring the security of the device's RF performance, manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download RF-controlling software, electronic signatures in such software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

[4] For U-NII devices certified as Software Defined Radio (SDR), see KDB Publication 442812 D01.

II. SOFTWARE SECURITY DESCRIPTION GUIDE

An applicant must 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.[5] While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards for security.[6]

This guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization.

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.
	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?
	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.
	4. Describe in detail any encryption methods used to support the use of 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?
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.
	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

[5] An exhibit that is part of the "Operational Description" can be treated as confidential. Applicants may request that the software description, as part of the operational description exhibit type, be held confidential. If the software description is submitted as the software information exhibit, it is automatically held confidential.

[6] For these purposes, it is suggested that manufacturers may consider existing security standards and definitions: X.800, RFC 2828, and IEEE 802.11i.

	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.
	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.[7]

III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.[8]

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?[9]
	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?
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

[7] Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (*See*, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.

[8] *See* KDB Publication 594280 D01Software Configuration Control for Devices. The document provides guidance for devices permitting device configurations and limitations on configuration parameters accessible to the third-parties in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the RF parameters of the Software Defined Radio (SDR).

[9] The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output 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.

	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?
	(2) What controls exist so 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?
	(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?
	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.
	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?
	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))

CHANGE NOTICE

07/10/2014: 594280 D02 UNII Device Security v01 has been replaced by 594280 D02 UNII Device Security v01r01. Changes made to items 3 and 4 in the Software Configuration Description table.

03/18/2015: 594280 D02 UNII Device Security v01r01 has been replaced by 594280 D02 UNII Device Security v01r02. Changes made to questions in General Description and Third Party Access sections of the Software Security Description table.

11/12/2015: 594280 D02 UNII Device Security v01r02 has been replaced by 594280 D02 UNII Device Security v01r03. Changes made to questions in “Third Party Access” section of the Software Security Description table and to clarify the applicability to software controlling RF parameters.