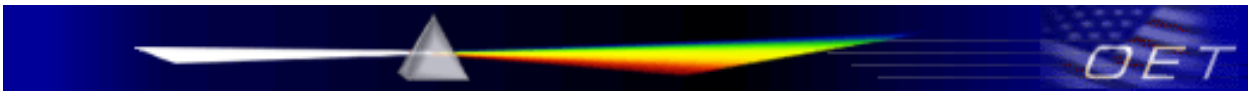

Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

August 14, 2014

GUIDANCE ON SOFTWARE OR NETWORK CONFIGURATION OF NON-SDR DEVICES TO ENSURE COMPLIANCE

I. GENERAL CONSIDERATIONS

Many radio frequency transmitters rely on software based configurations to ensure compliance with the Commission's rules.[1] § 2.931 requires the grantee to ensure that the product as marketed complies with the conditions of the grant under all circumstances and any software used to configure the transmitter cannot be modified or used in manner such that will cause the device to be out of compliance. For professionally installed equipment or modular transmitters, properly authorized installers and integrators may adjust the output power, as long as the radiated power is within the range authorized in the grant, for the antenna used in a specific installation.

Section 2.944 (b) requires that any ". . . radio in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the operating parameters of frequency range, modulation type or maximum output power … or the circumstances under which the transmitter operates in accordance with Commission rules" must comply with the requirements of Software Defined Radio (SDR). For the purposes of these rules, a third-party is anyone except the grantee; such third-parties include end users, service providers, operating system providers, application developers, Other/Original Equipment Manufacturer(s) (OEM) integrators, professional installers or authorized service dealers. For, any non-SDR device a third-party is not permitted to modify the operating parameters of frequency range, modulation type, maximum output power or the circumstance under which the transmitter has been approved.

Further, user accessible software either through direct access or by a software download must not enable any operation which modifies the operating parameters of the device beyond its equipment authorization. However, under certain circumstances, the Commission rules permit limited configuration in the field by software upgrades or permit a device to operate under control of a master which may provide configuration information to a radio transmitter (client device) to operate in a compliant manner.

The following sections provide further guidance for operation under different operational conditions.

[1] The term "software" is used generally in this context. Many different approaches may be used to store and manage operations configuration of a radio frequency transmitter. These may include configurations based on using Read-only-Memories (ROM), field programmable ROM, firmware used to boot devices, BIOS control, software drivers loaded on system start, sensor based controls, network management systems, external database controls, service provider controls, user interface controls, etc.

II. PROFESSIONAL INSTALLER AND SERVICE PERSONNEL CONFIGURATION CONTROLS

In many cases, a radio frequency transmitter requires professional installation or requires authorized service personnel to configure the transmitter. In such cases installers may be allowed access to the configuration parameters for adjusting power or location information to accommodate local installation; but only the specific configuration parameters identified in the equipment authorization may be programmed on-site.[2] However, on-site adjustments using country code parameters are not permitted to select the transmitter's frequency of operation, or to program other technical parameters such as Dynamic Frequency Selection (DFS) used for radar detection.

The rules in Parts 80, 90 and 95 permit service personnel to have limited access to configure devices to operate on licensee's frequency bands of operation.[3] In such cases it is permissible for the device to have password control, to software, that authorizes service personnel to configure such device. These password based controls can be implemented by the grantee through a web-based authentication procedure or require the service personnel to set the password by resetting the factory based default configuration. The "operations description exhibit" associated with the application for certification of such devices must clearly describe the control procedures implemented to ensure that only service personnel have access to the programming capabilities. The end users in all these cases must not be able to program the radios.

III. USER CONFIGURATION CONTROL

The Commission rules generally require that radio frequency devices do not provide user configuration control either through configuration screens or other means. For example, § 15.15(b) prohibits any user control of parameters; §§ 90.203(g) and 90.427(b) restrict options through front panel programming and §§ 95.645(g) and 95.655 place similar restrictions on user controls. In particular, users must not be relied on to set a country code or location code to ensure compliance. It is not sufficient to have this information provided in the user's manual or operations guide. For devices relying on geo-location capabilities as required by the rules or permitted under certain conditions, the grantee must implement adequate protection measures to ensure that such capabilities cannot be by-passed through user interface options or third-party application downloads.

IV. CLIENT DEVICE OPERATIONS CONTROL

In many networking applications a master transmitter may control how other transmitters operate by providing control as well as network related information. In such cases the ability of the devices to ensure compliant operation may depend on the information provided by the master device and the reliability of the information provided. As discussed below, under certain circumstances, the operation of the devices may be based on the information obtained from a master or other geo-location source.

A. Part 15 Devices

§ 15.202 of the rules requires that master devices marketed within the United States be limited to operation on permissible Part 15 frequencies, and such devices cannot have the ability to be configured by end users or professional installers to operate outside the authorized bands. Such

[2] Currently only Mode 1 Television Band Devices (TVBDs) authorized under Part 15 Subpart H permit a professional installer to program the location information for compliance purposes.

[3] § 80.203(b) also places similar restrictions.

devices must not have the option to set or select country codes or permit similar configuration options through software parameters for different regulatory domains to configure the device transmitter power or frequency or other technical parameters. It is permissible to allow the selection of different regulatory domains, if the transmitter operates only in bands with technical requirements permitted by the Commission rules, and in compliance with the certification as granted irrespective of the programmed regulatory domain.

A client device is defined in § 15.202 as "a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network." Any device meeting the definition of a client as specified in § 15.202 may have the ability to operate on other regulatory domain frequencies if it is under the control of a certified master device. Applications for such client devices must clearly include information that the device performs only passive scanning to detect a master device prior to initiate a transmission.

If a device is approved as a master in certain bands and as a client in other bands, the grantee must ensure that there are no software updates or capabilities that will allow the device to operate outside its authorized capabilities in the U.S. for each approved band. Applications for such devices must include in its operations description exhibit how the device ensures proper operation in each band.

B. Wi-Fi® Client Devices[4]

As discussed above, a client device cannot initiate, or be configured to initiate, any transmission including probes, beacons, or ad hoc mode transmissions. Many devices referred to by the Wi-Fi industry as "client devices" may not meet the definition of a § 15.202 client. Such devices must be approved as master devices on the bands for operation in U.S., and must operate in accordance with the grant conditions. Under certain circumstances a Wi-Fi device may be approved as a client device if it operates under the control of an approved master device.

1. Wi-Fi Devices operating in Channels 12 and 13

In the U.S., Wi-Fi devices operating on channels 12 and 13 (in 2.4 GHz band under § 15.247 rules) must ensure that the maximum transmit power is properly adjusted to comply with the out-of-band emission requirements.[5] A Wi-Fi client device that relies on a network access point to determine if it can operate on channels 12 and 13 must ensure that its transmission will comply with the rules when operating in the U.S.[6] If a Wi-Fi client device has the ability to operate at different power levels, it is not sufficient to use passive scanning alone, in order to meet the U.S. and non-U.S. requirements. The client device must use a supplemental approach to ensure compliance while operating on these channels. At minimum, the device must have the following capabilities:

(a) Device must, by default, operate in a mode that is compliant with the U.S. requirements.

(b) Device must use supplemental information such as geo-location data to determine that it is operating outside the U.S., if necessary, to change its power. Such supplemental data must be

[4] Wi-Fi® is a registered trademark of Wi-Fi Alliance®.

[5] *See* § 15.247.

[6] Typically this is done by "passive scanning". In this case the device scans to determine the channels used by an access point for communications to establish a network connection.

derived from one or more of the following:

(1) Global Navigation Satellite System (GNSS)[7] sensors in the device, or

(2) Mobile Country Code (MCC),[8] or MCC with a Mobile Network code (MNC), received from a CMRS[9] carrier and received directly by a receiver on the device,[10] or

(3) Country information derived from multiple adjacent access points (for example using IEEE Std 802.11d provisions) may be permitted on case-by-case basis,[11] or

(4) Other suitable geo-location data based on IP addresses or other reliable source.

(c) Device must recheck the geo-location information at least once every hour, when the device is switched on and connections are established or changed.

Equipment authorization applications, for such devices, must include an operational description of how such location information is obtained and controlled. The test report must include verification and validation that the selected geo-location procedures are functioning properly. A device that only does passive scanning and operates on channels 12 and 13 without using supplemental information to confirm location and without meeting the U.S. emission requirements cannot be approved.

Equipment authorization applications for devices relying on IP address based geo-location data or country information derived from adjacent access points are subject to Permit-but-ask procedures. The submission for such application must provide sufficient details about how the data is collected, managed and include reliability of the data.[12]

For modular transmitters and peer-to-peer applications, see the discussion below (see V, IV.B.3).

2. Wi-Fi Devices operating in 5.2 and 5.4 GHz band

All devices operating in the 5.2 and 5.4 GHz bands are subject to the requirement of U-NII rules of Part 15 Subpart E. All devices acting as master under the definition of § 15.202 must also have radar detection capabilities. Wi-Fi Client devices capable of peer-to-peer applications or *ad hoc* communications must be approved as a master device with radar detection unless they operate under conditions discussed below (see IV.B.3). Devices that support "Wi-Fi Hotspot"

[7] GNSS includes GPS or other similar Satellite navigation systems or A-GPS capabilities.

[8] Currently the U.S. has at least three valid Mobile Country Codes for use with its networks. Mobile Network Code alone is not and adequate solution for geo-location data.

[9] Commercial Mobile Radio Service (CMRS) bands includes devices typically operating in the cellular, PCS, AWS and ESMR bands under appropriate rules in Parts 20, 22, 24, 27 and 90.

[10] The device must compare MCC information from multiple base stations, whenever possible and select the code transmitted by maximum number of base stations to avoid selecting the wrong code, in particular, at U.S. borders.

[11] Client device must receive country information agreement from multiple access points and specific protocol for use of this approach must be pre-approved by the FCC. IEEE Std 802.11d-2001 was incorporated into and replaced by IEEE Std 802.11-2007; at present IEEE Std 802.11-2007 is replaced by IEEE Std 802.11-2012.

[12] The information must also include how the IP address based geo-location works when a device uses remote desktop configurations or Virtual Private Network (VPN) access.

capabilities in a smartphone or other CMRS devices must be approved as master devices and are subject to the Dynamic Frequency Selection (DFS) requirements including radar detection function.[13]

3. Wi-Fi Devices with Peer-to-Peer communications

A device that supports *ad hoc* or "peer-to-peer" networking modes typically initiates a connection without a network master. This includes devices that support Wi-Fi Direct® Group Owner modes and Tunneled Direct Link Setup (TDLS) modes specified by Wi-Fi Alliance®.[14] Such devices generally must be approved as master to meet all the requirements of §§ 15.247 and 15.407, as appropriate. Devices approved to operate on Wi-Fi channels 12 or 13 must clearly show compliance with the emission requirements of § 15.247 and devices approved under § 15.407 must have radar detection functionality and Dynamic Frequency Selection (DFS) capabilities.

Wi-Fi devices may be approved as a client device to support peer-to-peer or *ad hoc* communications if under all operating conditions they operate under the control of a master device. In this case the Wi-Fi client devices must operate in the same band and channel as network master (or the Access Point) with which they are associated. Wi-Fi client devices that do not maintain full association with the access point may be permitted to operate as "listen-only" clients if they meet certain criteria. The "listen-only" clients must implement a protocol that ensures that both members of a peer-peer connection are listening to the same access point, that at least one of the parties is fully associated with the master and that they have a timer or other mechanism to determine if the master is no longer active on the channel. If any of the conditions are not met the device must stop transmitting in the band. Client devices must ensure that they can and are permitted to "listen" to a master and that the control information is not encrypted in order to be able to use this mode of operation.[15]

For devices operating on Wi-Fi channels 12 and 13, the devices must ensure, through supplemental determination, that if they are in the U.S. that they operate at the permissible power levels.

Equipment authorization applications for such devices must include in operational description how the device maintains association with a master and must include test results showing that the devices change channels according to the channel change announced by the associated master.

C. CMRS Subscriber Devices

CMRS subscriber devices typically operate under the control of a base station in the CMRS bands.[16] In general, compliance for such devices is based on the licensee's authorized frequencies of operation. Devices containing bands of operation not available in U.S. may be authorized as long as proper declarations are included in the equipment authorization application filings. However, with increasingly complex capabilities of the devices and different operating modes (both U.S. and non-

[13] *See* § 15.407.

[14] Wi-Fi Direct is specified by Wi-Fi Alliance to enable direct device to device communications. *See* http://www.wi-fi.org/Wi-Fi_Direct.php. Wi-Fi Direct® and Wi-Fi Alliance® are registered trademarks of Wi-Fi Alliance.

[15] The protocol for such client devices must be pre-approved by the FCC. *See* KDB Publication 388624 D02.

[16] Subscriber devices generally operate under the license issued to a network operator. *See* § 1.903(c).

U.S.) on the same or overlapping bands it may be necessary to configure the devices by software or network control to ensure compliance with the Commission rules. Certification of such device operation modes are permitted under certain conditions as discussed here.

1. Devices using Mobile Country and Mobile Network codes

In general devices may not use MCC and MNC codes to configure or determine operating restrictions for compliance in the U.S. However, if the device's default operation mode is for compliant operation in the U.S., it may be reconfigured to operate outside the U.S. in other modes when it receives either a non-U.S. MCC or a non-U.S. MCC with a non-U.S. MNC, directly from a network carrier.[17] The MNC alone is not sufficient for determining operation outside the U.S. The device must check the country and network codes at least once every hour and anytime the device operation is reset or when a connection is initiated or changed. If a valid code is not received or if conflicting codes are received the device must remain in or reset to, the default mode for compliance with operation in the U.S. If the device is able to check the information from multiple base stations, it must choose the country code transmitted by a majority of the base stations. If it cannot resolve the conflict the device must default to mode for compliance with operation in the U.S. Devices may use geo-location capabilities, as a complimentary feature, to ensure that the device is operating in the U.S. and use that information to configure it for compliance with the U.S. regulations. Currently the most common geo-location capability is to use GNSS capabilities. If such capabilities are used they must be available all the time while the devices are operational without the ability of end user disabling, or a "safe" mode of operation should be enabled if the capabilities are unavailable. A "safe" mode of operation is either a mode compliant for operation in the U.S. or a no-transmission mode.

Equipment authorization applications for such devices must include a clear operational description of how this feature works including a description of failsafe mechanisms to address reception of conflicting codes within U.S. The test reports must include results showing proper device operation with the use of MCC and MNC and under fail-safe operational modes. The device must show compliance with all the Commission's technical requirements in the default mode.

If the devices rely on additional network signaling to configure power levels to comply with the Commission's technical requirements, this should be included in the operational requirements and test results must include data showing compliance with that configuration.

2. Devices with Extended Frequency Capabilities

Many devices are approved under multiple rule parts where operating frequencies overlap U.S. and non-U.S. allocations. Such approvals are noted with "extended frequency" grant notes.[18] For devices with such extended frequency of operation, the equipment authorization application must clearly include a description of the methods used to ensure such compliance.

[17] The Mobile Country and Mobile Network Codes must actually be received from the network carrier and not from a stored data in the device or subscriber modules.

[18] *See* KDB Publication 634817. Test results for operation of the device on frequency bands not authorized or approved in U.S. must not be included in the filings.

V. MODULAR TRANSMITTERS AND HOST BASED CONTROL

In many networking applications a master transmitter may control how other transmitters operate by providing control as well as network related information. In such cases the ability of the devices to ensure compliant operation may depend on the information provided by the master device and the reliability of the information provided. As discussed below, under certain circumstances, the operation of the devices may be based on the information obtained from a master or other geo-location source.

A. Modular Transmitters for Wi-Fi Client Devices

Modular transmitters for Wi-Fi Client devices which will rely on network information must receive the appropriate information from the host platform in secure manner.

1. Wi-Fi Transmitter operating in Channels 12 and 13

As discussed in IV.B.1, if a transmitter for integration into a Wi-Fi client device has the ability to operate at different power levels and it uses passive scanning in order to meet the U.S. and non-U.S. requirements, then it must use supplemental approach to ensure compliance while operating on these channels. The supplemental information sensors may be on the modular transmitter or the information may be derived from the host. The modular transmitter and the host combined must have the capabilities as outlined in IV.B.1 with the addition that the software driver for control of the modular transmitter used by the host must be provided by the grantee or approved by the grantee to ensure secure and reliable operation of the module. The control information from the host to the client must not be accessible to third parties.

Equipment authorization applications for such devices must include in the operational description how the location information is obtained, controlled and managed. The test reports must include test data for the device in the default mode and any changes with the supplemental geo-location data. The grantee must include a description of how the module will validate the input from the host.[19] Equipment authorization applications for such modular transmitters relying on IP address based geo-location data or country information derived from adjacent access points are currently subject to Permit-but-Ask procedures.

2. Wi-Fi Transmitters Operating in 5.2 and 5.4 GHz Band

Modular transmitters operating in the 5.2 and 5.4 GHz bands are subject to the requirement of U-NII rules of Part 15 Subpart E. All modular transmitters for integration into hosts for operation as master under the definition of § 15.202 must also have radar detection capabilities. Modular transmitters for integration into hosts for operation as Wi-Fi Client devices and intended for use for peer-to-peer applications, *ad hoc* communications or as "Wi-Fi Hotspot" must be approved as master devices with radar detection unless they operate under conditions discussed below.

3. Wi-Fi Transmitters with Peer-to-Peer Communications

Modular transmitters for integration in a host device that supports *ad hoc* or "peer-to-peer" networking modes including Wi-Fi Direct Group Owner modes and TDLS modes specified by

[19] For modular transmitters using IP address based geo-location the applicant must provide sufficient details about how the data is collected, managed and include reliability of the data when the devices may use remote desktop access or work over Virtual Private Networks (VPNs).

Wi-Fi Alliance must be approved as master and must meet all the requirements of §§ 15.247 and 15.407, as appropriate. As discussed above, transmitters approved to operate on Wi-Fi channels 12 or 13 must clearly show compliance with the emission requirements of § 15.247 and devices approved under § 15.407 must have radar detection functionality and Dynamic Frequency Selection (DFS) capabilities.

Modular transmitters may be approved for integration with a client device to support peer-to-peer or *ad hoc* communications if they operate under the control of a master device. In this case the transmitter must operate in the same band and channel as the network master (or the Access Point) with which they are associated. Wi-Fi client devices that do not maintain full association with the access point may be permitted to operate as "listen-only" clients if they meet certain criteria. The "listen-only" clients must implement a protocol that ensures that both members of a peer-peer connection are listening to the same access point, that at least one of the parties is fully associated with the master and that they have a timer or other mechanism to determine if the master is no longer active on the channel. If any of the conditions are not met the device must stop transmitting in the band. Client devices must ensure that they can and are permitted to "listen" to a master and that the control information is not encrypted in order to be able to use this mode of operation.[20] Equipment authorization applications, for such devices, must include in operational description exhibit how the device maintains association with a master and must include test results to show that the device changes channel as the associated master changes channel.

Modular transmitters operating on Wi-Fi channels 12 and 13 using passive scanning the devices must ensure through supplemental determination that if they are in the U.S. that they operate at the permissible power levels. Equipment authorization applications for such devices must include in the operational description how such the location information is obtained and controlled. The test reports must include data showing that the device operates properly in the default mode and for any power changes when the device is supposed to be operating outside the U.S. The grantee must include a description of how the module will validate the input from the host. Equipment authorization applications for such modular transmitters are currently subject to Permit-but-Ask procedure.

B. Modular Transmitters for CMRS Subscriber Devices

Modular transmitters for CMRS subscriber devices, where permitted for certain host platforms or configurations, must meet all the requirements for client devices discussed in IV.C.

VI. PERMISSIVE CHANGES AND FIELD PROGRAMMING

Procedures applicable to a Class II permissive change are described in KDB 178919. Under certain circumstances, where a non-SDR device has been modified, a grantee may be permitted to enable devices deployed in the field through "over-the-air" programming. The Commission may also allow grantees to permit specific parties, such as operating system providers, service providers or parties under direct control of the grantee to enable software upgrades for field deployed non-SDR devices. Such upgrades can be permitted with connection to the grantee's or related party's website. The details of such arrangements including the procedures to maintain control of the software uploads must be included in

[20] The protocol for such client devices must be pre-approved by the FCC. *See* KDB Publication 388624 D02.

the original filing or Class II permissive change filings and are subject to the Permit-but-ask procedures for TCB processing.[21]

VII. DOCUMENTATION REQUIREMENTS

Applications for equipment authorization for non-SDR transmitters that have software configuration control for radio parameters, or other technical parameters as reported to the Commission to ensure compliance, must provide a technical description of how such control is implemented to prevent third-party modification and to ensure the device only operates within the parameters of the grant of authorization. If the device supports any of the options for client devices or other devices discussed above, the operational description must include how the device permits such operation and what controls are included to ensure continued compliance. In addition, as required, the test report must include data showing compliance of the device operating in the default mode and any other power change condition modes. If the device depends on supplemental input to determine its location for ensuring compliance the operation of this mode must also be clearly included in the supporting documentation.

VIII. RELATED AND/OR CITED KDB PUBLICATION NUMBERS AND TITLES

KDB 178919, PERMISSIVE CHANGE POLICY.

KDB 388624, D01 PERMIT BUT ASK PROCEDURE, D02 PERMIT BUT ASK LIST.

KDB Publication 594280 D02 U-NII Device Security provides general guidance on the type of information that should be submitted in the equipment authorization application in order to demonstrate compliance with the Software Security Requirements for U-NII Devices.

KDB 634817, FREQUENCY RANGE LISTINGS FOR CERTIFICATION GRANTS.

Change Notice

02/24/2011: KDB Publication 594280 was changed on 02/24/2011. Prior to this change this publication did not contain any attachments. This change moved the general guidance on Restrictions on Software Configuration for devices not approved as Software Defined Radios into an attachment. In addition, guidance was added regarding restrictions on permissive changes through software exceptions referencing KDB 178919 Permissive changes.

06/08/2011: 594280 D01 Software Configuration Control v01 has been changed to 594280 D01 Software Configuration Control v01r01 for clarification for applications for equipment authorization for non-SDR transmitters has been added.

10/24/2012: 594280 D01 Software Configuration Control v01r01 has been changed to 594280 D01 Software Configuration Control v01r02. Removed for the requirement for Non-SDR to file a Class II permissive change directly with the Commission.

06/02/2014: 594280 D01 Software Configuration Control v01r02 has been changed to 594280 D01 Software Configuration Control v02. This is a major revision of the previous version.

[21] *See* KDB Publication 388624 for Permit-but-ask and KDB Publication 178919 regarding restrictions on permissive changes through software or any exceptions.

08/14/2014: 594280 D01 Software Configuration Control v02 has been changed to 594280 D01 Software Configuration Control v02r01. Modified language for “listen only” client devices; and added conditions for MCC use near the U.S. border.