Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Brandon

Last Name: Fosso

Mailing Address: 1413 18th Ave N

City: Minneapolis

Country: United States

State or Province: MN

ZIP/Postal Code: 55411

Email Address: brandonfosso@gmail.com

Organization Name:

Comment: Hi, thanks for taking my comment. I was brought to this site by an article posted on the website Hackaday and read about the proposed changes in a document entitled SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES and dated March 18, 2015. My understanding of said document is that the FCC seeks to compel future ID applicants to "lockdown" the radio firmware on said device. (Please forgive any misuse of terms, I am no expert :) Based on my own experience with testing radios to FCC regulation, I suspect that this is meant to curtail abuses of channel usage and transmit power in the U-NII band. While this is generally a good idea, I think the solution of locking down firmware goes, unintentionally, too far. My worry it that in our haste to prevent malicious usage of the spectrum, we will destroy the user's ability to configure the wired network to their liking via custom firmware. As a specific example, let us consider a router in which the cpu doing the routing for the Ethernet switch also controls/configures the radio. Based on my reading of the FCC document, I would think that under the new rules, one would be prevented from modifying the firmware running on the router cpu. This would prevent the user from installing open-source firmware like openWRT. Such firmware can be used to optimize the home network for greater productivity while reducing electronic waste via greater hardware longevity. These are great things! and I do not want to see them killed in the name of

protecting the spectrum. Transmitting above the legal power limit and operating on forbidden channels is wrong but surely we can find a way to police these things short of locking down device firmware. Thanks for reading!

Hi, thanks for taking my comment. I was brought to this site by an article posted on the website Hackaday and read about the proposed changes in a document entitled SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES and dated March 18, 2015. My understanding of said document is that the FCC seeks to compel future ID applicants to "lockdown" the radio firmware on said device. (Please forgive any misuse of terms, I am no expert :) Based on my own experience with testing radios to FCC regulation, I suspect that this is meant to curtail abuses of channel usage and transmit power in the U-NII band. While this is generally a good idea, I think the solution of locking down firmware goes, unintentionally, too far. My worry it that in our haste to prevent malicious usage of the spectrum, we will destroy the user's ability to configure the wired network to their liking via custom firmware. As a specific example, let us consider a router in which the cpu doing the routing for the Ethernet switch also controls/configures the radio. Based on my reading of the FCC document, I would think that under the new rules, one would be prevented from modifying the firmware running on the router cpu. This would prevent the user from installing open-source firmware like openWRT. Such firmware can be used to optimize the home network for greater productivity while reducing electronic waste via greater hardware longevity. These are great things! and I do not want to see them killed in the name of protecting the spectrum. Transmitting above the legal power limit and operating on forbidden channels is wrong but surely we can find a way to police these things short of locking down device firmware. Thanks for reading!