Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: William

Last Name: Bechtold

Mailing Address: 2515 Fairhill Drive

City: Cincinnati

Country: United States

State or Province: OH

ZIP/Postal Code: 45239

Email Address: wmichaelb@fuse.net

Organization Name: null

Comment: I must respectfully but firmly ask that the FCC NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices, for several reasons:

1.) Any computing device networking system is dependent for its security on the ability of researchers to investigate, modify, and test their devices. Most of this work is now done by researchers who do not work for the equipment manufacturers. That work would not be able to be continued if the rules prevent it.

2.) Most manufacturers offer limited times of warranty at best. The rules as proposed will force users to purchase new equipment at best. There are many examples of software errors that end users have been able to patch that were not fixed by the manufacturer of the equipment.

3.) Many billions of dollars of commerce in systems such as secure wireless vendors, retail hot spot vendors, and university or other campus wireless systems vendors are at risk if those who install and maintain their systems cannot update or modify the software for their own uses.

4.) Most security bugs are found and patched far faster when users and researchers are involved than could possibly be done with changes in hardware.

The United States is at cyber war with many forces around the world. Do not put us at greater risk by forbidding us to defend ourselves!

I must respectfully but firmly ask that the FCC NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices, for several reasons:

1.) Any computing device networking system is dependent for its security on the ability of researchers to investigate, modify, and test their devices. Most of this work is now done by researchers who do not work for the equipment manufacturers. That work would not be able to be continued if the rules prevent it.

2.) Most manufacturers offer limited times of warranty at best. The rules as proposed will force users to purchase new equipment at best. There are many examples of software errors that end users have been able to patch that were not fixed by the manufacturer of the equipment.

3.) Many billions of dollars of commerce in systems such as secure wireless vendors, retail hot spot vendors, and university or other campus wireless systems vendors are at risk if those who install and maintain their systems cannot update or modify the software for their own uses.

4.) Most security bugs are found and patched far faster when users and researchers are involved than could possibly be done with changes in hardware.

The United States is at cyber war with many forces around the world. Do not put us at greater risk by forbidding us to defend ourselves!