

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: Shay

Last Name: Walters

Mailing Address: 1327 S Beltline Blvd.

City: Columbia

Country: United States

State or Province: SC

ZIP/Postal Code: 29205-4913

Email Address: shayw@controlmanagement.com

Organization Name:

Comment: I would like to comment on "ET Docket No. 15-170; RM-11673" and address the proposed changes that would require manufacturers to restrict the ability of end users to modify devices they have purchased.

It has been a pervasive problem that manufacturers react to security or operational issues of many devices (such as internet routers) within a very brief timeframe after a device has been released. New security exploits arise constantly, leaving many devices vulnerable to being exploited by nefarious parties. There are a small number of third-party firmware developers who have developed, and continue to maintain, firmware or software that is able to address new security risks. These include the DD-WRT and Open-WRT projects.

Requiring manufacturers to restrict the ability of end-users to load such software into their devices will leave the end-users vulnerable to any new security risks that have arisen after the brief timeframe during which manufacturers release updated firmware.

I would like to comment on "ET Docket No. 15-170; RM-11673" and address the proposed changes that would require manufacturers to restrict the ability of end users to modify devices they have purchased.

It has been a pervasive problem that manufacturers react to security or operational issues of many devices (such as internet routers) within a very brief timeframe after a device has been released. New security exploits arise constantly, leaving many devices vulnerable to being exploited by nefarious parties. There are a small number of third-party firmware developers who have developed, and continue to maintain, firmware or software that is able to address new security risks. These include the DD-WRT and Open-WRT projects.

Requiring manufacturers to restrict the ability of end-users to load such software into their devices will leave the end-users vulnerable to any new security risks that have arisen after the brief timeframe during which manufacturers release updated firmware.