

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: Ron

Last Name: Watkins

Mailing Address: 6003 Wellworth Ave

City: Chattanooga

Country: United States

State or Province: TN

ZIP/Postal Code: 37412

Email Address: null

Organization Name: null

Comment: This is an extraordinarily bad idea, and will have frightening worldwide security implications.

The current radio firmware market is a mess. The whole industry is in a perpetual rush to market, with very little aftermarket support. Most current radios are software driven, meaning they need firmware loaded to be operational. It's like all software, in that if it's done in a hurry, it's probably not going to be very good, and there's probably no market moving faster than wireless devices. Vendors abandon these products very quickly, but the bugs remain on devices in service, sometimes for multiple years.

The open source community is able to fix many of the problems. Not all of them, of course, but the impact has been quite noticeable, and the industry has been moving more and more to an open source approach, where customers can take over where the company leaves off. Individual customers are frequently quite motivated to get security patches deployed, in essence doing some of the ongoing maintenance work for free, so releasing open source drivers for many of these radios makes a great deal

of sense on all sides. Companies get free maintenance work, and customers get security fixes even after their hardware has been abandoned. These proposed rules will shut that down. Very likely, what will happen is a steady spread of severe security holes, even to the point that even other government agencies may be unable to secure their networks properly... or if they can, it will be more expensive to do so, because they'll have to pay for ongoing firmware support that the open source people would have done for nothing.

The nature of software is that it's hard to write, and very hard to debug, but it's easy to copy once it's been created. It makes a lot of sense to cooperate in creating it; a few people working together can make (or debug) something great, and then give it to everyone at just about zero additional cost, perhaps recruiting even more help from other interested users. (this snowball effect is what created Linux, which is heavily used all through government.) It's a huge value multiplier, and this proposed ruling will ensure that this scenario can't happen in radio. This nascent software industry will die. The knock-on consequences will be dire and long-lasting, even to the point that it may affect the individuals in the FCC directly. Not too many years down the road, your systems may be compromised via a wireless security flaw that you indirectly caused with these proposed rules!

Security is really hard, and sharing the load is critical to doing it well. Please, please don't wreck this industry. It doesn't sound like the problems with unlicensed transmissions have been *that* serious, while the proposed remedy will have enormous side effects, most of which you probably haven't considered.

At the very least, I'd suggest putting the US on notice that this kind of rule change might be required if we don't collectively get our acts together. If, in a couple years, you haven't seen real progress in self-policing, then it might make more sense to look into hardware lockdown, but this absolutely should not be your first solution. The costs will be dire, and will stretch across decades.

Thanks for your attention.

This is an extraordinarily bad idea, and will have frightening worldwide security implications.

The current radio firmware market is a mess. The whole industry is in a perpetual rush to market, with very little aftermarket support. Most current radios are software driven, meaning they need firmware loaded to be operational. It's like all software, in that if it's done in a hurry, it's probably not going to be very good, and there's probably no market moving faster than wireless devices. Vendors abandon these products very quickly, but the bugs remain on devices in service, sometimes for multiple years.

The open source community is able to fix many of the problems. Not all of them, of course, but the impact has been quite noticeable, and the industry has been moving more and more to an open source approach, where customers can take over where the company leaves off. Individual customers are frequently quite motivated to get security patches deployed, in essence doing some of the ongoing maintenance work for free, so releasing open source drivers for many of these radios makes a great deal of sense on all sides. Companies get free maintenance work, and customers get security fixes even after their hardware has been abandoned. These proposed rules will shut that down. Very likely, what will happen is a steady spread of severe security holes, even to the point that even other government agencies may be unable to secure their networks properly... or if they can, it will be more expensive to do so, because they'll have to pay for ongoing firmware support that the open source people would have done for nothing.

The nature of software is that it's hard to write, and very hard to debug, but it's easy to copy once it's been created. It makes a lot of sense to cooperate in creating it; a few people working together can make (or debug) something great, and then give it to everyone at just about zero additional cost, perhaps recruiting even more help from other interested users. (this snowball effect is what created Linux, which is heavily used all through government.) It's a huge value multiplier, and this proposed ruling will ensure that this scenario can't happen in radio. This nascent software industry will die. The knock-on consequences will be dire and long-lasting, even to the point that it may affect the individuals in the FCC directly. Not too many years down the road, your systems may be compromised via a wireless security flaw that you indirectly caused with these proposed rules!

Security is really hard, and sharing the load is critical to doing it well. Please, please don't wreck this industry. It doesn't sound like the problems with unlicensed transmissions have been *that* serious, while the proposed remedy will have enormous side effects, most of which you probably haven't considered.

At the very least, I'd suggest putting the US on notice that this kind of rule change might be required if we don't collectively get our acts together. If, in a couple years, you haven't seen real progress in self-policing, then it might make more sense to look into hardware lockdown, but this absolutely should not be your first solution. The costs will be dire, and will stretch across decades.

Thanks for your attention.