



November 9, 2015

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
455 12<sup>th</sup> St. SW  
Washington DC 20554

RE: **EX PARTE** in Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment, ET Docket 15-170

Dear Ms. Dortch:

Several parties in the above-captioned proceeding have questioned whether the proposed rules would in some way exclude the use of Open Source software in radios. Cisco supports rules that would allow open source software to be used, and sees nothing in the proposed rules that would bar the use of Open Source software in FCC authorized transmitters. The issues raised in the comments may misunderstand what Cisco believes the Commission's view to be, and why the Commission arrived at its proposed view. In this *ex parte*, Cisco offers the following as information in the hope this will inform the debate.<sup>1</sup>

**Open Source software can be used to fulfill the Commission's proposed requirements to lock down RF emissions in a band.**

The Commission has long required that the applicant for an FCC ID for a Software Defined Radio show that RF emissions cannot be altered by the end user. This requirement ensured that radios would operate as authorized, minimizing the possibility of interference that would be presented if radios operated at higher power, in disregard of emissions masks, etc. Minimizing interference is also important in conserving the Commission's enforcement resources, as well as in ensuring a given radio band is available to those authorized to use it. In the above-captioned proceeding, the FCC is recognizing that virtually all radio emissions in modern radios are controlled by software, and is proposing to extend its previously enacted rule to unlicensed devices generally. Particularly for Part 15 devices, these

---

<sup>1</sup> Cisco has not met with FCC personnel. Cisco elected to file an *ex parte* in lieu of a reply comment, as the content of this filing is primarily intended to be informational.

transmitters increasingly operate in bands where there are incumbent users that are protected by decisions the FCC has made about the unlicensed RF emissions.

There is nothing in the Commission's existing or proposed rules that would limit or eliminate the ability of a developer to use Open Source software, including software that controls radio emissions. Open Source relates to the availability to review and reuse source code. This review process can be beneficial to developers of technology in many ways, including those seeking to manage risk and mitigate security vulnerabilities. The ability to review source code is not inherently incompatible with the notion of locking the integrity of a product against modification or tampering. It is perfectly possible for a product to have source code that is capable of review by the public while that same code is secured inside the device against change by the end-users. In fact, the Department of Defense published an extensive FAQ document in 2010 to address myths around the security implications of using open source software.<sup>2</sup>

To begin, Open Source software can be understood to mean the following:

**Open-source software (OSS)** is computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.<sup>[1]</sup> Open-source software may be developed in a collaborative public manner. [https://en.wikipedia.org/wiki/Open-source\\_software](https://en.wikipedia.org/wiki/Open-source_software)

The specific bundle of rights available to the public may vary depending upon the particular license selected by the developer. There are a wide range of OSS licenses with variations in what rights they confer.

An important distinction to be drawn here is the difference between OSS and the resultant products being produced leveraging that OSS. In many commercial products, companies leverage OSS in their product and, as long as the associated OSS license permits, then implement both technological and contractual/legal means that prevent end users from modifying the software.

Commonly, commercial products developed using OSS licenses --- as compared with collaborative community developed projects --- are packaged, engineered and designed in ways that explicitly work to prevent unauthorized modification of the software while its deployed in the product. Among other reasons, this is done so that the buyers/users of the software are assured the software will perform as expected, and that any underlying data will not be jeopardized.

---

2

[http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx#OSS\\_and\\_Security.2FSoftware\\_Assurance.2FSytem\\_Assurance.2FSupply\\_Chain\\_Risk\\_Management](http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx#OSS_and_Security.2FSoftware_Assurance.2FSytem_Assurance.2FSupply_Chain_Risk_Management)

In general, the security goal of Open Source developers (and proprietary software developers alike) is to “raise the cost” of malicious attacks so that potential hackers will move on to find a different target of vulnerability. Open Source developers can modify existing code and add new security features – and publish those back to the Open Source community. For example, the developer of a radio handset may appropriate a block of existing open source code, modify it for use inside the radio and then publish the resulting changes back to the library for that open source module so that others may examine the code, spot flaws, or develop further enhancements. If further modifications are made to that same block of code by other open source developers, the radio developer may---or may not---choose to incorporate the subsequent version of that code back into the developers software release for the radio.

A portion of the Open Source community would likely prefer developers to provide the source code inside the device to be open and readable, but also intentionally modifiable in the end implementation. Hobbyists may, for example, develop prototype devices using Open Source hardware and software, such as “Arduino.” End users of such devices, which are designed for tinkerers, may modify the source code and then upload changes into the device. And so long as the modifications do not involve RF emissions under the proposed FCC rule, there would be no bar to such modification. However, it is important to recognize that end user modification is not a mandatory property of open source development, nor is OSS necessary for ‘tinkerer’ platforms. It is perfectly compatible with the notion of Open Source software for the code to be available for review and secured against changes inside of a specific device, application or service such that the technology performs only as the developer intended---or in the case of a regulatory environment as the government approved.

The pervasive use of Open Source software testifies to the ability of developers to design defenses against malicious attacks, and improve upon them over time. Open Source today is widely used in enterprises and by government in a wide variety of applications. As noted above, the Department of Defense has published an FAQ about the use of open source software that addresses security myths associated with this method of developing code. When the White House moved to use an open source development system called “Drupal” in 2009, the code used to run “Drupal” could be inspected by public. But that did not render the content of the White House website open to being edited by the general public. As one commentator noted at the time. “it's perfectly possible to use open-source software in a system that's locked-down and closed.”<sup>3</sup>

As further noted in a 2011 OMB memo by then CIO Vivek Kundra, Administrator for Federal Procurement Policy, Dan Gordon, and U.S. Intellectual Property Enforcement Coordinator Victoria Espinel the federal government should consider all licensing models in its own procurements and acquisitions of technology. “The

---

<sup>3</sup> <http://www.cnet.com/news/white-house-web-site-makes-open-source-move/>

policies in these documents are built around the use of merit-based requirements development and evaluation processes that promote procurement choices based on performance and value, and free of preconceived preferences based on how the technology is developed, licensed or distributed. In the context of developing requirements and planning acquisitions for software, for example, this means, as a general matter, that agencies should analyze alternatives that include proprietary, open source, and mixed source technologies. This allows the Government to pursue the best strategy to meet its particular needs.”<sup>4</sup>

**Geolocational tools to ensure RF emissions remain in compliance with national rules are a strong complement to using software, but are not a substitute.**

Geolocational tools are increasingly offered by manufacturers to help ensure that radio transmitters are being operated within national rules. While initially these tools allowed user selection of jurisdiction, the Commission ultimately found that users’ selections were sometimes at odds with where the radio was located, resulting in interference and the need for enforcement action. For that reason, geolocational tools are migrating to mechanisms that the user cannot manipulate, following the Commission’s new thinking on reducing user discretion. However, these improved geolocational tools remain a complement to requirements to lock down those portions of software code that affect RF emissions. Simply put, if you remove user discretion to select jurisdiction, but allow end users to readily change RF emissions through software, you haven’t done much to address potential interference cases.

**Key to FCC’s ability to allow shared use of bands (e.g., where other services or uses are present) is strongly aided by software-upgradable RF emissions to reflect future rules changes or to address issues that might arise.**

Particularly with respect to bands that are shared, such as portions of the 5 GHz band that share with governmental radars, it is almost unthinkable to deploy unlicensed devices into a band whose RF parameters cannot be changed in the future. Not only might the Commission’s rules change, but incumbent operations might change, necessitating changes to transmission rules for unlicensed devices. Moreover, should interference caused by an unlicensed transmitter occur, the ability of a manufacturer to upgrade devices in the field to correct the issue is invaluable – to all stakeholders. In all these cases, new software loads can avoid the delay, expense and hardship of ripping out a radio network and installing a brand new one.

---

4

[https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/memotociostechnologyneutrality.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf). A list of U.S. government documents relating to the use of open source software can be found here: <http://opensourceforamerica.org/learn-more/federal-open-source-policies/>

While replacing hardware might sound like an alternative to a software upgrade, it is not a comparable exercise. Hardware replacement raises significantly more issues for a network administrator.

Moreover, embedding RF emissions in hardware is an inefficient and problematic policy choice. Should a regulator wish to change the rules due to an unanticipated interference problem, the regulator is confronted with the decision whether to try to find and replace radios that have been in the marketplace – often for years. Finding those radios is not simple. Nor is the customer going to be happy at the prospect of having to pay for new hardware. Policies that avoid difficult, contentious and unsuccessful product recalls are a better way forward, and provide confidence that shared use of bands can be better managed.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: Mary L. Brown  
Senior Director, Government Affairs  
601 Pennsylvania Ave. NW 9<sup>th</sup> Fl. North  
Washington, D.C. 20004  
(202) 354-2923