Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Facilitating Opportunities for Flexible, Efficient,	)	
and Reliable Spectrum Use Employing Cognitive	)	ET Docket No. 03-108
Radio Technologies	)	

SECOND MEMORANDUM OPINION AND ORDER

Adopted: January 14, 2010 **Released: January 19, 2010**

By the Commission:

I. INTRODUCTION

1. By this action, we dismiss a petition for reconsideration filed by the SDR Forum[1] requesting that the Commission modify the policy statements it made in the *Memorandum Opinion and Order (MO&O)* in this proceeding[2] concerning the use of open source software to implement security features in software defined radios (SDRs).[3] While we are dismissing this petition on procedural grounds, as discussed below, we also are providing clarification concerning the issues raised therein.

II. BACKGROUND

2. On March 17, 2005, the Commission adopted the *Cognitive Radio Report and Order* in which it modified its rules to reflect ongoing technical developments in cognitive and software defined radio (SDR) technologies.[4] Specifically, the Commission: 1) eliminated the rule that a manufacturer supply radio software (source code) to the Commission upon request; 2) required that a manufacturer supply a high level operational description of the radio software that controls the transmitter's RF characteristics in the application for certification of a software defined radio; 3) clarified the rules to permit manufacturers to market radios that have the hardware-based capability to transmit outside authorized United States frequency bands, but have software controls to limit operation to authorized frequency bands when used in the United States; 4) broadened the definition of SDR to include devices designed such that a software change could modify not only the operating parameters of frequency range, modulation type or maximum output power, but also the circumstances under which a transmitter

[1] SDR Forum, Petition for Reconsideration, filed July 3, 2007.

[2] *See Memorandum Opinion and Order* in ET Docket No. 03-108, 22 FCC Rcd 8053 (2007).

[3] A software defined radio is a transmitter in which the operating parameters of frequency range, modulation type or maximum output power, or the circumstances under which the radio transmits in accordance with the rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions. *See* 47 C.F.R. § 2.1. Open Source Software (OSS) is software in which the source code is made available for others to study, use, modify and/or redistribute. Some parties use the term Free Software (FS) rather than OSS to describe such software because parties are free to study, use, modify and/or redistribute to the code. GNU/Linux is a widely used OSS operating system and is sometimes referred to simply as Linux.

[4] *See Report and Order* in ET Docket No. 03-108, 20 FCC Rcd 5486 (2005).

operates in accordance with the rules; 5) modified the rules to require that radios with software that is designed or expected to be modified by a party other than the manufacturer have reasonable security measures to prevent unauthorized modifications that would affect the RF operating parameters or the circumstances under which the transmitter operates in accordance with Commission rules; and 6) described the technical measures that cognitive radios could employ to allow secondary use of spectrum by lessees while maintaining the availability of the spectrum for a higher priority use by the licensee when needed.

3. On April 20, 2007, the Commission adopted the *MO&O* which responded to two petitions filed in response to the *Cognitive Radio Report and Order*.[5] The Commission, *inter alia*, granted a petition for clarification filed by Cisco Systems, Inc. ("Cisco") requesting that the Commission clarify: 1) the requirement to approve certain devices as software defined radios; and 2) its policy on the confidentiality of software that controls security measures in software defined radios.

4. In responding to the Cisco petition, the Commission stated that with regard to the use of open source software for implementing software defined radio security measures:

> "…manufacturers should not intentionally make the distinctive elements that implement that manufacturer's particular security measures in a software defined radio public, if doing so would increase the risk that these security measures could be defeated or otherwise circumvented to allow operation of the radio in a manner that violates the Commission's rules. A system that is wholly dependent on open source elements will have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio."[6]

5. The SDR Forum filed a petition for reconsideration on July 3, 2007 requesting that the Commission modify these statements. Their petition is discussed below.

III. DISCUSSION

6. In its petition, the SDR Forum expresses concern that the language in the *MO&O* on the use of open source software for implementing SDR security measures may inadvertently pose a barrier to the development and wide implementation of security techniques that would ensure compliance with the Commission's rules. It recommends that these policy statements be modified, stating that manufacturers should have the discretion to discuss their security measures in public so long as the intent of the disclosure is not to enable circumvention of the Commission's rules. The SDR Forum states that the Commission should remain neutral on the security of open source elements because open source approaches are no less secure than proprietary techniques. It specifically requests that the Commission modify the text quoted above by: 1) revising the first sentence to state "a manufacturer may make public its SDR security mechanisms so long as the intent is not to circumvent compliance with Commission rules;" and 2) deleting the second sentence.

7. In support of its petition, the SDR Forum makes several arguments. First, it argues that an attempt to achieve security by keeping the methodology confidential, which it termed "security through obscurity," often fails because that approach precludes a broad and rigorous review that would uncover its flaws and enable experts to fix shortcomings. The SDR Forum states that if the security of a

[5] *See supra* n. 2. The Commission granted in part and denied in part a petition for reconsideration filed by Marcus Spectrum Solutions ("MSS"). Specifically, the Commission: 1) clarified that its rules did not require the submission of radio software source code; 2) clarified the rules concerning the certification of software defined amateur radio equipment; and 3) declined to initiate a further proceeding to adopt regulatory requirements for high-power, high-speed digital-to-analog (D/A) converters.

[6] *See MO&O* at 8056.

software defined radio depends on the confidentiality of a security method provided to the Commission, a product recall may be required to restore security whenever information in the certification application to the Commission is revealed. It believes that the information that should remain secret in the security framework are keys, passwords and biometric data that provide various forms of access control. It argues that the Commission should place less emphasis on the confidentiality of security methods and instead focus on the standards that assure confidentiality of cryptographic secrets in operation.

8. The SDR Forum expresses concern that the policy of prohibiting disclosure of security information to third parties may discourage standardization of security methods that would be in the public interest. It claims that the revelation of a security approach would enable others to scrutinize it and make improvements to it. The SDR Forum states that the Commission's order implies radio security mechanism development and radio manufacturing are vertically integrated, but it believes that for the most effective techniques to be implemented across SDR markets, security mechanisms need to be shared across multiple manufacturers. Therefore, it believes that manufacturers will likely need to "intentionally make the distinctive elements that implement…security measures in an SDR public."

9. Finally, the SDR Forum states that while there is active debate on the security posture of open source software, considerable evidence exists that open source code typically is more secure than proprietary code because open source code is exposed to a wide range of experts with an interest in the success of the software and the willingness to update it to correct known flaws. It contends that if the Commission continues to pursue a "high burden" for open source elements, it will be drawn into discussions of what these terms mean. The SDR Forum believes that the Commission should remain neutral with respect to open source security methods, and that academic inquiry and industry discussion coupled with a market test are more likely to lead to the correct outcome with respect to the open source debate than regulatory intervention.

10. We are dismissing the SDR Forum petition for reconsideration on procedural grounds. While the SDR Forum filed comments in response to the *Notice* in this proceeding, it did not submit comments in response to the Cisco petition for reconsideration that raised the issue of using open source software to implement software defined radio security mechanisms. The Cisco petition was addressed in the Commission's *MO&O* for which the SDR Forum now requests reconsideration. A petition for reconsideration that relies on facts not previously presented to the Commission will be granted only if: 1) the facts relied on relate to events which have occurred or circumstances which have changed since the last opportunity to present them to the Commission; 2) the facts relied upon were unknown to the petitioner until after his last opportunity to present them to the Commission, and the petition could not through the exercise of due diligence have learned of the facts in question prior to such opportunity; or 3) the Commission determines that consideration of the facts relied on is required in the public interest.[7] The SDR Forum petition does not address why it did not respond to the Cisco petition or claim that any of these three conditions are met in this case. Accordingly, the SDR Forum's petition for reconsideration is procedurally defective and is hereby dismissed. However, we recognize that the issue of open source software in software defined radios is of interest to the SDR Forum and other parties. Accordingly, we are taking this opportunity to clarify the Commission's policies with respect to the use of open source software for implementing security features in software defined radios.

11. The Commission's rules require that a software defined radio manufacturer take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio. The software must not allow the user to operate the transmitter with radio frequency parameters other than those that were approved by the Commission. The Commission's rules require that the manufacturer have reasonable security measures to prevent unauthorized modifications that would affect

[7] *See* 47 C.F.R. § 1.429(b).

the RF operating parameters or the circumstances under which the transmitter operates in accordance with Commission rules. Manufacturers may select the methods used to meet these requirements and must describe them in their application for equipment authorization.[8]

12. When a party applies for certification of a software defined radio, the description of the security methods used in the radio is automatically held confidential.[9] We do this because such information often is proprietary and also because revelation of the security methods, or portions thereof, could possibly assist parties in defeating the security features and enable operation of the radio outside the Commission's rules. Out of an abundance of caution – because operation of a radio outside the Commission's rules could result in harmful interference to a wide variety of radio services, including safety-of-life services – the Commission holds the entire description of the security measures confidential. Therefore, the Commission's staff does not have to determine which portions of a software defined radio security methods description filed with an application could be made publicly available without risk that such disclosure could assist parties in defeating the security measures. Further, by automatically holding the description confidential, applicants for certification do not have to specifically request confidentiality for the description of a radio's security mechanisms.

13. Neither the Commission's rules whereby it maintains the confidentiality of a software defined radio's security mechanism nor the policy stated in the *MO&O* prohibit radio manufacturers and software developers from sharing information on the design of security methods with other manufacturers and developers. Rather, the Commission's policy stated only that manufacturers should not make the "distinctive elements" of security features publicly available, if doing so would increase the risk that security measures could be defeated or circumvented to allow operation of a radio in a manner that violates the rules. The Commission's intent was not to prohibit manufacturers from collaborating and sharing information that could allow them to develop more robust security features or reduce the cost of implementing them. In fact, we would encourage such work by industry. The Commission's concern is only with disclosure of those particular elements of a security scheme when such disclosure could facilitate defeating the security scheme. Thus, manufacturers can make whatever information they wish concerning their security methods public, provided they can demonstrate the implementation has a means of controlling access to the distinctive elements that could allow parties to defeat or circumvent the security methods.

14. We wish to emphasize that the Commission does not prohibit the use of open source software in implementing software defined radio security features. The Commission's concern with open source software is, as stated above, that disclosure of certain elements of a security scheme could assist parties in defeating the scheme. As Cisco stated in its petition, licensing agreements may require that open source software code be made publicly available. This could potentially lead to public disclosure of this information. For these reasons, the Commission stated in the MO&O that a system that is wholly dependent on open source elements would have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio. However, the Commission's statements in the MO&O were not intended to prohibit the use of open source software or discourage its use. All applicants seeking to certify a software defined radio are held to the same standard, *i.e.,* they must demonstrate that the radio contains security features sufficient to prevent unauthorized modifications to the radio frequency operating parameter. A party applying for certification of a software defined radio would need to show that public disclosure of the source code would not assist parties in defeating the security scheme, or that disclosure of the distinctive elements of the security scheme would not assist parties in defeating it. As the SDR Forum notes, security mechanisms can rely on a variety of means to control access, such as keys, passwords or biometric data.

[8] *See* 47 C.F.R. § 2.944.

[9] *See* 47 C.F.R. §0.457(d)(1)(ii).

15. Finally, as software defined radio and security technologies continue to develop and mature, the Commission may address the rules for software defined radios, including their security requirements, in future proceedings. We encourage the SDR Forum and other interested parties to participate in such proceedings.

IV. ORDERING CLAUSES

16. Accordingly, IT IS ORDERED that the petition for reconsideration filed by the SDR Forum IS HEREBY DISMISSED. This action is taken pursuant to the authority contained in Sections 4(i), 301, 302, 303(e), 303(f), and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. Sections 154(i), 301, 302, 303(e), 303(f), and 303(r).

17. IT IS FURTHER ORDERED that ET Docket No. 03-108 IS TERMINATED.

18. For further information regarding this Second Memorandum Opinion and Order, contact Mr. Hugh L. Van Tuyl, Office of Engineering and Technology, (202) 418-7506, e-mail Hugh.VanTuyl@fcc.gov.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary