SDR FORUM COMMENTS TO FCC IN THE MATTER OF FACILITATING OPPORTUNITIES FOR FLEXIBLE, EFFICIENT, AND RELIABLE SPECTRUM USE EMPLOYING COGNITIVE RADIO TECHNOLOGIES *AND* AUTHORIZATION AND USE OF SOFTWARE DEFINED RADIOS

SDRF-04-A-0004-v0.00

(FORMERLY SDRF-04-I-0041-v3.01)

APPROVED 1 MAY 2004

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
	)	
Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies	)	ET Docket No. 03-108
	)	
	)	
Authorization and Use of Software Defined Radios	)	ET Docket No. 00-47
	)	

COMMENTS OF THE SOFTWARE DEFINED RADIO FORUM

The Software Defined Radio Forum (SDR Forum) is an international, non-profit organization dedicated to promoting the development, deployment and use of software defined radio (SDR) technologies. More than 125 organizations throughout the world are members of the SDR Forum.[1] Participants in SDR Forum activities are decision-makers, planners, policy-makers, technologists, educators, and managers from a wide variety of commercial, educational, scientific and governmental organizations.

BACKGROUND

Software defined radio is a rapidly evolving technology that will bring enormous benefits to the providers and consumers of wireless services. The potential of SDR technology is well known to this Commission, which has aggressively reformed its rules in a way that has helped allow SDR technology to become a reality. As it continues to develop, SDR technology will also play an important role in the development of

[1] *See* http://www.sdrforum.org/sdrf_members.html.

cognitive radios and in the fullest possible exploitation of the spectrum resource. Thus, the SDR Forum supports the Commission's effort to promote the development of cognitive radio technology.

The SDR Forum is also aware of the Commission's concern about the potential for the misuse of SDR technologies by criminals. Developing security to protect against such misuse is a central part of the SDR Forum's mission. Indeed, it sponsors an ongoing effort to encourage the development of ever more robust methods for protecting the security of software defined radios and for authenticating radio software.

Because the private sector has itself an enormous incentive to develop robust security to protect against the misuse of software defined radios – and because it has developed robust security measures – the SDR Forum has generally cautioned the Commission (and other regulators) to refrain from mandating security rules that could interfere with the realization of SDR's full potential. In earlier proceedings before this Commission, the SDR Forum suggested that no special rules on security safeguards were needed for software defined radios.[2] But in light of the Commission's continuing concerns about security, and the experience industry has had with the technology over the past few years, the SDR Forum believes it is an appropriate time to reassess the issue of security safeguards.

In this proceeding, the Commission has suggested that the security issue be addressed by mandating that manufacturers "declare" certain kinds of equipment to be SDRs,[3] and by imposing security and other obligations once such a declaration is made.

---

[2] *See* SDR Forum Comments in ET Docket No. 00-47 at p. 14.

[3] *See Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies, Authorization and Use of Software Defined Radios,* Notice of Proposed

While the SDR Forum understands – and to some degree shares – the Commission's concerns about security, it believes this approach is overbroad and will have adverse consequences for the growth of the technology. Instead, the SDR Forum believes it makes more sense to impose a narrowly targeted security obligation on radios whose operating parameters can be remotely programmed and whose hardware is capable of transmitting in public safety[4] bands or the restricted bands.[5]

DISCUSSION

The Commission first adopted special rules for SDR technology in 2001.[6] As noted in this NPRM, those rules were designed to make it easier for manufacturers to deploy SDR technologies by streamlining the approval process for radios with operating parameters that could be modified by software changes. The primary "streamlining" was the elimination of the need to re-label a device in the field with a new FCC ID number after the radio's operating parameters were changed by a change in its software. To take advantage of this option, a manufacturer would have to declare a device to be an SDR

Rulemaking and Order, 18 FCC Rcd. 26859 (rel. December 30, 2003) at¶88. Currently, an "SDR declaration" is permissive.

4 "Public safety" includes not only those bands regulated by the FCC in 47 CFR Part 90, but also those Government bands regulated by the NTIA and used for critical Federal functions including DOD, FAA, those Federal agencies with emergency management, emergency medical, fire suppression, and law enforcement responsibilities, etc.

5 The restricted bands appear in 47 C.F.R. §15.205. Generally, certain emission levels are not permitted in these bands in order to protect sensitive government operations.

6 The initial SDR rules where developed in ET Docket No. 00-47. In that proceeding, the Commission noted that it would consider further rule changes in the future as SDR technology advances. *See Authorization and Use of Software Defined Radios,* First Report and Order, 16 FCC Rcd. 17373 (rel. September 14, 2001) at ¶5.

when it applied for equipment certification.[7] Any device declared to be an SDR would then be subject to certain obligations, including the obligation to incorporate security features ensuring that only software in an approved hardware/software combination is used.[8] The Commission did not, however, require all devices meeting its definition of an SDR to be declared to be "SDRs." Nor did it require manufacturers to incorporate security protections into software defined radios that were not declared to be SDRs.

I. A MANDATORY SDR DECLARATION COMBINED WITH THE BROAD DEFINITION OF AN SDR WILL CREATE UNNECESSARY BURDENS ON MANUFACTURERS

In this NPRM, the Commission seeks comment on whether manufacturers should be required to "declare certain equipment as SDRs."[9] The Commission is concerned that manufacturers of software defined radios are not declaring them to be SDRs and, thus, are not obligated to incorporate security mechanisms. It notes that with the SDR rules now two years old, no one has sought to certify a device under SDR rules.[10] The Commission reasons that by requiring all devices that meet its definition of a software defined-radio to be declared as SDRs, it would force manufacturers to incorporate security mechanisms "minimiz[ing] the possibility of unauthorized operation of software programmable radios[.]"[11]

---

7 NPRM and Order at ¶83. The Commission also adopted a number of other rule changes for SDR-designated devices, including an electronic display of FCC identification numbers and an obligation to provide a copy of the device's operating parameter control software upon request.

8 *See* 47 C.F.R. §2.932(e).

9 NPRM and Order at ¶88.

10 NPRM and Order at ¶84.

11 NPRM and Order at ¶88.

The problem with this approach is that the term "software defined radio" can cover a wide range of devices. As the Commission has recognized, its definition of a software defined radio is extraordinarily broad.[12] It defines a software defined radio as one in which "operating parameters such as the frequency and modulation type are determined by software."[13] This would include, for example, private land mobile radios, most PCS base stations and many traditional cell phones. The SDR Forum itself uses a broad definition of the term, considering software-defined radios to be "radios that provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communication security functions (such as hopping), and waveform requirements of current and evolving standards over a broad frequency range."[14] But the security concerns raised by the Commission here have little or nothing to do with most radios that are covered by these broad definitions. Thus these security concerns can be addressed without requiring manufacturers to declare all software defined radios as SDRs. Moreover, because the definition of a software defined radio is so broad, a mandatory SDR declaration will force manufacturers to declare as SDRs many radios that have no need for the streamlined modification procedures. This would create a large and unnecessary burden for manufacturers, and turn the original intent of the SDR designation – the elimination of unnecessary burdens – on its head.

---

12 *See* NPRM and Order at ¶84.

13 *Authorization and Use of Software Defined Radios*, First Report and Order, 16 FCC Rcd. 17373 (2001). More completely, it defines a software defined radio as one "that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions." *Id*. at 17375.

14 *See SDR Primer,* Software Defined Radio Forum, http://www.sdrforum.org/sdr_primer.html.

II. THE COMMISSION SHOULD FOCUS ITS EFFORTS ON PREVENTING SOFTWARE DEFINED, REMOTELY PROGRAMMABLE TRANSMITTING DEVICES FROM UNAUTHORIZED TRANSMISSIONS ON CRITICAL FREQUENCIES

The SDR Forum does not dismiss the FCC's security concerns about software defined radios. But the real issue is not whether a device fits the broad definition of a software defined radio. Rather, the issue is whether a device incorporates functionalities that would require the Commission to apply special security rules to that device.

The Commission's real security concern here is not (or should not be) that a particular radio can be modified to operate in a way that violates the Commission's rules. It has always been true that individual radios could be modified to operate on frequencies or in a manner for which they have not been authorized. This generally requires no more than a pair of pliers, a soldering iron, and a little knowledge about how a radio works. This kind of radio-by-radio rule violation, while not acceptable, has never been a large-scale problem for other spectrum users or the Commission – simply because the number of radios affected was not significant. That a radio's operating parameters may be embedded in software rather than hardware does not itself change this equation. Today, the operating parameters of most software defined radios can be changed only if someone sits next to that radio and reprograms it. This kind of radio-by-radio rule violation too, while not acceptable, does not pose a large-scale problem for other spectrum users or the Commission – simply because the number of radios potentially affected is not significant.

The Commission's real security concern is (or should be) that large numbers of radios could be modified simultaneously. *This means the Commission need focus its attention only on radios whose transmitting parameters can be remotely changed by a software download, since that is where the risk exists.* And this risk is worthy of

regulation only where the radios have hardware enabling them to operate in public safety or restricted bands. For this reason, the SDR Forum believes the correct security approach is for the Commission to clarify the security responsibilities and obligations of manufacturers who develop and seek authorization of software defined radios that are remotely programmable and that are hardware capable of transmitting on public safety or restricted frequency bands.

III. THE COMMISSION SHOULD ADOPT MANDATORY SECURITY ONLY FOR SOFTWARE DEFINED, REMOTELY PROGRAMMABLE RADIOS THAT ARE CAPABLE OF TRANSMITTING IN PUBLIC SAFETY OR RESTRICTED BANDS

The SDR Forum believes that the unauthorized operation of large numbers of radios in public safety or restricted bands would be a serious problem. It also believes, however, that this potential problem can be fully addressed by requiring parties seeking authorization of software defined, remotely programmable radios with hardware capable of transmitting in those bands to meet certain security and software authentication requirements. The SDR Forum also believes that those parties should be required at the time of equipment authorization to certify the sufficiency of their security safeguards.

Manufacturers of declared SDR devices are now required under Section 2.932(e) of the Commission's rules to "take steps to ensure that only software that has been approved with a software defined radio can be loaded into such a radio." It also provides that "manufacturers may use authentication codes or any other means to meet these requirements."[15] The SDR Forum believes that it would be appropriate for the Commission to apply this requirement to all software defined remotely programmable radios that are capable of transmitting in public safety or restricted bands – regardless of

[15] *See* 47 C.F.R. §2.932(e).

whether they are declared as SDRs. But, as before, the Commission should not mandate the specific security measures taken.

Section 2.932(e) also requires manufacturers of declared SDR devices *to describe* to the Commission in their applications for equipment authorization the methods used to ensure that only approved software can be loaded into their radios. The SDR Forum suggests that – if the disclosure concerns noted below are addressed – these provisions also be applied to all software defined remotely programmable devices that are capable of transmitting in public safety or other restricted bands. Further, the Commission could require that manufacturers submitting such devices for equipment authorization file with the Commission a certification that the appropriate security and authentication safeguards are in place. Should the Commission find the certification inaccurate or inadequate, the device would not receive an authorization. Alternatively, if this deficiency is found post-authorization, the device would be found to be in non-compliance. These steps, if adopted, would address the Commission's security concerns, without burdening manufacturers in a way that would deter the development and deployment of SDR technology. Moreover, the Commission would not need to require that devices be declared SDRs. That designation can continue to be voluntary, as it is today. Nor would the Commission need to define the specific methods of software downloads to which SDR security requirements apply.[16]

IV. TO PROMOTE THE SECURITY AND DEPLOYMENT OF SDR TECHNOLOGY TCB'S SHOULD BE ALLOWED TO CERTIFY SOFTWARE DEFINED RADIOS

There is one other step the Commission could easily take to promote the deployment of SDR technology and to protect the security of that technology. As noted

[16] *See* NPRM and Order at ¶88.

above, current rules require manufacturers of declared SDR devices to disclose the security methods being used to protect their radios against unapproved software. And the SDR Forum has conditionally suggested extending that obligation to any software defined, remotely programmable radio that is capable of transmitting in public safety or restricted bands. But the *public* disclosure of such security methods could actually be used to undermine those security methods. There may also be commercial reasons to avoid the public disclosure of security methodologies. Indeed, the requirement to describe security methods to the Commission may well be one of the factors deterring manufacturers from declaring devices as SDRs.

It is possible, of course, for a manufacturer to request confidentiality from the Commission. But the process for doing so can be itself lengthy, and a grant of confidentiality is not guaranteed. Moreover, there have been a number of occasions where confidential information submitted to the Commission has accidentally been posted on its public website.

There is, however, an easy fix for this problem. It is routine for manufacturers to disclose sensitive information to designated Telecommunication Certification Bodies (TCBs). Manufacturers seeking equipment certifications often provide such sensitive information to TCBs pursuant to contracts that protect against disclosure. The protection of sensitive information in such cases is fast and automatic, and the information is virtually immune from accidental disclosure. TCBs could also be used to protect the security measures required to be disclosed for declared SDRs or for any software defined, remotely programmable radios. But, under the existing SDR rules, manufacturers are prohibited from using TCBs for SDR authorization. Thus the SDR Forum suggests

permitting TCBs to be used for the authorization of all software defined radios. This will provide manufacturers more comfort about disclosing their security methods and further the Commission's goals of promoting both the deployment and security of SDR technology.

CONCLUSION

SDR technology truly has enormous potential. It can play an important role in the development of cognitive radios, the development of secondary spectrum markets, and the more efficient use of the spectrum resource. It can also be used to reduce costs for manufacturers and for consumers. And it can be especially useful in a variety of critical public safety and other governmental applications.

But the potential also exists that some software defined radios could be remotely altered to interfere with public safety and other sensitive communications. A mandatory SDR declaration requirement is not the way to thwart this potential problem. Instead, the SDR Forum believes the Commission can avert potential risks to public safety and restricted spectrum by adopting a simple security and certification obligation for software defined radios that both are remotely programmable and able to operate in the public safety or restricted bands.

Respectfully submitted,

By: _____
Scott Blake Harris
Damon Ladson*

HARRIS, WILTSHIRE & GRANNIS LLP
1200 EIGHTEENTH STREET, N.W.
WASHINGTON, D.C. 20036
(202) 730-1300

3 May 2004

Counsel for the SDR Forum

* Technology Policy Advisor