

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

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 (Terminated)
)	

To: The Commission

**COMMENTS OF THE
NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL**

The National Public Safety Telecommunications Council (“NPSTC”) hereby respectfully submits the following Comments in response to the Commission’s *Notice of Proposed Rule Making and Order*, FCC 03-108 (released December 30, 2003) (“*NPRM*”), in the above-captioned proceeding.

With over 74,000 public safety organizations in the United States, it is critical to have a resource and an advocate for public safety telecommunications. That is the primary role of the National Public Safety Telecommunications Council. NPSTC is a federation of public safety associations that encourage and facilitate, through a collective voice, the implementation of Public Safety Wireless Advisory Committee (PSWAC) and 700 MHz Public Safety National Coordination Committee (NCC) recommendations. NPSTC explores emerging public safety telecommunications issues and technologies, and develops recommendations to appropriate governmental bodies to support the broad goals of promoting public safety telecommunications

worldwide. Finally, NPSTC serves as a standing forum for the exchange of ideas and information regarding public safety telecommunications. NPSTC currently consists of the following thirteen organizations:¹

- American Association of State Highway and Transportation Officials
- American Radio Relay League
- American Red Cross
- Association of Public-Safety Communications Officials-International
- Forestry Conservation Communications Association
- International Association of Chiefs of Police
- International Association of Emergency Managers
- International Association of Fire Chiefs
- International Association of Fish and Wildlife Agencies
- International Municipal Signal Association
- National Association of State Emergency Medical Services Directors
- National Association of State Telecommunications Directors
- National Association of State Foresters

¹ A number of Federal agencies are affiliate members of NPSTC and active participants in its ongoing efforts. These include the Department of Agriculture, Department of Homeland Security (SAFECOM Program and Federal Emergency Management Agency), and Department of the Interior.

TABLE OF CONTENTS

Indexed by Paragraph Number

INTRODUCTION	1
GENERAL VIEWS AND ISSUES	3
<i>Role of Software and Software Defined Radio (SDR)</i>	4
<i>Risks Are Inherent and Must be Addressed</i>	5
<i>Definitions and Terminology</i>	7
SAFEGUARDS TO MANAGE SOFTWARE-DEFINED TRANSMITTERS	10
<i>Safeguards a Major Theme in SDR and now Cognitive Radio (CR)</i>	10
<i>Security/Authentication for SDR Devices</i>	13
<i>Alternative Approach to Safeguards via "Umbrella Coverage"</i>	14
HIGH-POWERED UNLICENSED DEVICES IN RURAL MARKETS	17
SECONDARY MARKETS	19
<i>Access/Reversion Mechanisms</i>	20
OTHER APPLICATIONS OF COGNITIVE RADIO	23
<i>Facilitating Interoperability</i>	23
<i>Dynamically Coordinated Spectrum Sharing</i>	25
<i>Mesh Networks</i>	26
<i>Frequency Selection for Unlicensed Devices</i>	27
EQUIPMENT AUTHORIZATION MATTERS	28
<i>Submission of Radio Software</i>	28
<i>Mandatory Declaration of SDR Devices</i>	29
<i>Other Considerations Relating to SDR</i>	31
<i>Applicability to Other Devices</i>	33
PRE-CERTIFICATION TESTING REQUIREMENTS	34
<i>Essential to Test Various Inputs and Combinations</i>	35
<i>Testing and Security Conformance a Vital Element of Public Spectrum Policy</i>	
<i>Proposed General Testing Framework for the Future</i>	37
CONCLUSIONS	39

I. INTRODUCTION

1. NPSTC acknowledges the tremendous demand of business, consumers, and Federal, State and local governments for wireless communications services and the rush to introduction of new and innovative technologies and techniques to satisfy these needs. The Commission is correct in its assessment that access and reliability, among other spectrum factors, are critical public policy issues, particularly with respect to the public safety sector. The efforts in this NPRM and related proceedings to use spectrum more intensively and improve efficiency are well directed as the primary means to satisfy the requirements of new services, rather than via the disruptive and slow-moving reallocations of the past. NPSTC concurs with the general FCC approach, i.e., "should not attempt to regulate cognitive radio technology in a way that could limit its potential," but additional rules relating to safeguards and security will be essential to achieve that goal.

2. The Commission is to be commended for its progressive and forward-looking steps to examine the role of advanced wireless technologies, such as cognitive radio (CR) and software defined radio (SDR), and the potential benefits for the future. In this regard, the Commission is urged to bear in mind several important aspects of public safety:

- A. For over a decade, public safety agencies have requested additional spectrum to ease life-threatening frequency congestion and enhance interoperability. Some of these requirements, particularly for spectrum supporting mission-critical voice communications, remain unsatisfied today in spite of the national emphasis on homeland security and the vital role of first responders. It may be possible that the spectrum access concepts presented in the NPRM could eventually assist in accommodating a small portion of these unmet requirements.

- B. Public safety has also recognized the need for spectrum and service rules that would facilitate implementation of new communications technologies. It appears that some of the specific techniques and applications described in the NPRM, such as mesh networks, will be beneficial to the community and could be developed and deployed in the foreseeable future.
- C. However, any potential benefits of these new technologies will be negated if they are implemented without a high degree of caution and consideration, such that existing public safety systems and other spectrum users are subjected to or even threatened by the risk of interference to operational systems. Every effort must be taken to ensure that new and unproven concepts do not cause adverse impact, or result in disruption due to accidental, intentional, malicious or otherwise avoidable actions related to the software-based nature of the new devices. With sufficient focus, analysis and testing, NPSTC believes it may even be possible to at least place boundaries around the "unforeseen" threat in deploying a future generation of wireless devices.

II. GENERAL VIEWS AND ISSUES

3. Advanced technologies are vital to the future of wireless communications, continued growth in services and applications, and ensured access to the radio spectrum. Inherent in virtually all new systems and techniques is a dominant software-based capability that can modify many critical characteristics of the device, including in many cases its RF parameters just as easily as its ring-tones and email applications. Cognitive radio will increasingly add the ability to sense, adapt and react to its unique environment, and achievement of an even broader range of benefits.

Role of Software and Software Defined Radio (SDR)

4. NPSTC concurs with the Commission's view that software and SDR will play a major role in many cognitive radio applications. It is readily apparent that SDR technology can assist or facilitate implementation of the several cognitive radio capabilities described in the NPRM, including frequency agility, adaptive modulation, and transmit power control, as well as the various applications presented, such as unlicensed devices, dynamic coordination, and interoperability.

Risks are Inherent and Must be Addressed

5. It is equally apparent to the Commission in this NPRM that the underlying software-based "smarts" of the cognitive radio, enabling a long list of potential benefits ranging from the user to the regulator, is also the source of great concern about the available security and safeguards associated with that software's use to modify RF parameters, thereby adding the risk of interference to other spectrum users. Just a few years ago, the Commission faced the same dichotomy in its proceeding on Software Defined Radio,² in which there were repeated acknowledgements of both benefits and risks.

6. Given that software configured radio is here to stay and will undoubtedly increase exponentially in the coming months and years, NPSTC urges the Commission to tackle the safeguard issue directly and decisively. Further, as proposed by the Commission in the present NPRM, NPSTC concurs that it is timely to revisit the SDR rules, rather than to fine-tune the security provisions for SDRs. The latter is much better handled by an alternative "umbrella safeguard approach" outlined later in these Comments.

² See *Authorization and Use of Software Defined Radios*, First Report and Order, 16 FCC Rcd. 17373 (rel. September 14, 2001).

Definitions and Terminology

7. It is noted that the Commission closed the SDR proceeding (ET Docket No. 00-47) and in so doing, raised a degree of confusion. On the one hand, the NPRM recognizes that a cognitive radio is not necessarily an SDR (NPRM at ¶10) – and vice versa – while later implying that "software defined radio" is included within the term "cognitive radio" (footnote 16). In practice, they are two quite distinct entities within the regulatory context; an SDR is a device and therefore falls mainly under the certification and authorization rules, while cognitive radio is a way to operate and hence relates to the technical and operating rules of the respective service. Clarification is requested.

8. More importantly, it is noted that the definition of SDR was a priority matter, whereas the Commission has no proposal or request for comment on a definition for cognitive radio. This NPRM (at ¶10) suggests it is a radio that can change its transmitter parameters based on interaction with the operating environment, while footnote 1 adds the aspect of learning or reasoning as a possibility. NPSTC considers it highly undesirable to leave the term vague in this manner, since features, capabilities, applications, sharing assumptions, testing conditions, and various other proposed rules will lack predictability if the possibility of "learning" is allowed to remain at this stage of development and deployment.

9. NPSTC, through its participation as the primary public safety representative to the SDR Forum, has had an opportunity to participate in many international discussions involving cognitive radio and SDR. After significant dialog with regulators in Canada and Europe, NPSTC suggests to the Commission that, at this stage in the introduction of these technologies, regulators desire a device whose operation is predictable in every case (a "policy-based radio") rather than one that could behave differently given the same environment due to learning from prior

experiences (“cognitive radio”). The Commission clearly understands the benefits of increased market size through international harmonization of devices and technologies, a trend that will be greatly enhanced by cognitive radio. However, such harmonization must begin with standardization of the basic definitions of these devices and technologies. The Commission is thus strongly urged to (a) consider adoption of recognized international definitions that clearly distinguish between the two possibilities, such as those for "policy-based radio" and "cognitive radio" under consideration in ITU-R SG8, and (b) to limit its current consideration to the former with regard to this NPRM.

III. SAFEGUARDS TO MANAGE SOFTWARE-DEFINED TRANSMITTERS

Safeguards a Major Theme in SDR and Now Cognitive Radio

10. As stated above, the Commission, in its SDR proceeding, repeatedly indicated concern about the security of software in the device and adequate safeguards to other spectrum users in the event of unauthorized use. The Commission finds itself repeating the same concerns with respect to cognitive radio and other devices that take advantage of software configuration of the transmitter. In the Notice, it asks whether current rules provide adequate safeguards against unauthorized changes to SDRs, and whether any changes are necessary to security and authentication requirements.

11. The issue is not whether a transmitter device is an SDR – formally declared or not – but rather, does the device have the potential to cause interference or similar adverse effects on other spectrum users because of the use of software to modify RF parameters of the radio after

manufacture. The concern relates to the use of unauthorized software, the prevention of unauthorized changes, or protection from interference caused by accidental, intentional, malicious and any other avoidable action caused by the software. It is clearly time to focus more directly on the core concerns, rather than the varying array of devices that incorporate software in rapidly growing numbers.

12. The Commission's real security concern should not be that a particular radio can be modified to operate in violation of the Commission's rules. Rather, the Commission's concern should be that large numbers of radios could be modified simultaneously, such as through a software download over the Internet or other connected network to remotely programmable devices resulting in a widespread disruption to other services, including interference to public safety services. It has always been true that individual radios could be modified to operate in an unauthorized manner. Indeed, there are publications available that provide detailed instructions on building a transmitter from parts, allowing it to operate however the builder chooses. While such radio-by-radio modification is neither legal nor desirable, it has never posed a large scale problem and the Commission, and indeed many public safety agencies, have effective methods for dealing with such cases. The fact that a radio's operating characteristics may be imbedded in firmware or software does not change this equation. The real risk to spectrum users is that a large number of radios, perhaps tens of thousands, could be simultaneously modified through a virus introduced into a commercial cellular system, or through devices interconnected to the Internet. For example, large networks such as those operated by NEXTEL and Southern LINC whose operational frequencies are interleaved with 800 MHz public safety assignments could be mass-reprogrammed over their own network to interfere with public safety operations by a hacker. Alternatively, wireless access points in the 5.1 GHz U-NII band that are interconnected

to the Internet could be attacked and mass-reprogrammed to operate in the adjacent 4.9 GHz public safety band. Thus, special attention must be given to these remotely programmable devices whose hardware is capable of transmitting in public safety bands³ and certain restricted bands.⁴

Security/Authentication for Software-Based Devices

13. The Commission asks whether more explicit rules are necessary to ensure security, such as requiring the use of electronic signatures to verify authenticity of software. It is well accepted that such signatures can and do provide a high level of computer security, when properly used in an overall integrated security solution. At the same time, the record of comments and the Commission's final Report and Order in the SDR proceeding clearly documented the undesirable aspects of mandating one or another of the candidate security schemes. Rather, there was broad consensus that the preferred approach was to rely on the manufacturer to design a security system drawing from all available means – hardware, software, computer security, or even signatures, coupled with the latest knowledge and guided by industry best practices. Nevertheless, NPSTC is convinced that it is time for the Commission to consider additional rules and/or guidelines for the near future, based on an alternative to the present SDR device-focused approach.

³ “Public safety bands” include 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.

⁴ The restricted bands appear in 47 C.F.R. §15.205 and include those protected by international treaty in footnote No. 5.340 of the ITU Radio Regulations which are used by passive services (RAS, ESS, and Space Research). Generally, certain emission levels are not permitted in these bands in order to protect sensitive government operations.

Alternative "Umbrella Coverage" Approach

14. NPSTC proposes that an alternative approach to safeguards be based on the assumption that any transmitter (or similar device, such as the high-speed DAC discussed in the NPRM) possessing the ability to modify its RF characteristics via remote software download be initially regarded as a potential candidate for consideration. It is conceivable that there may be a very small set of rules applicable to all such software-configurable devices, such as the need to isolate any software download from the RF section of the device or to prevent any virus from dialing a number as part of a major denial-of-service attack. Further, it will become obvious that large categories of systems and devices could be immediately ignored as a potential threat, e.g., no hardware capability to transmit in unauthorized spectrum. The goal is to focus on the entirety of the potential security threat and in so doing, to eliminate or diminish the chance of encountering an "unforeseen" spectrum disaster.

15. Notwithstanding the long-term importance of the broad approach, the most urgent task would be to focus on specific high-threat and/or high-risk situations. High-threat devices may involve the readily available and easily modified software radios off the Internet, which come complete with multiple waveforms and instructions, or systems capable of accessing very large numbers of software-controlled devices via remote download. High-risk situations would clearly include threats to the public safety and restricted bands. The immediate goal would be to develop and adopt specifically targeted rules that impose adequate security requirements in the near future and stringent pre-certification testing for security conformity.

16. The Commission has long-embraced the use of a Telecommunication Certification Body (TCB) to certify compliance of transmitting devices with appropriate FCC technical requirements. NPSTC suggests that TCBs, rather than the Commission itself, are the appropriate

mechanism to ensure that security requirements are properly implemented in remotely programmable transmitting devices whose hardware is capable of transmitting in public safety and restricted bands, based upon broad requirements established by the Commission. If the Commission itself was to provide such testing, we are concerned (a) that it would put an unnecessary burden on an already overtaxed Commission engineering staff that in all probability has minimum expertise in the software security area, and (b) that the security mechanisms employed to protect particular devices could be subject to public disclosure, thus potentially defeating the very basis of their being. Equipment manufacturers today routinely provide sensitive information to TCB's under non-disclosure contracts, providing effective assurance from public disclosure of such information. Thus, TCBs seem to be a logical choice to certify that security measures employed by particular transmitting devices meet the broad security requirements established by the Commission. Unfortunately, current rules do not permit SDR-declared transmitting devices to use TCBs for compliance certification. NPSTC contends that a relaxation of this restriction for SDRs would not only provide an improved mechanism to certify security protections, but would also provide regulatory relief to manufacturers.

IV. HIGH-POWERED UNLICENSED DEVICES IN RURAL MARKETS

17. NPSTC supports the underlying objectives of the Commission on this topic – to improve spectrum access and benefit consumers in rural areas – and it is conceivable that it may directly benefit the public safety community over time through the increased coverage and greater ranges provided. The proposed technical rules, sharing conditions, sensing requirements, and use of the

ISM bands appear well developed and present no specific threat to the primary public safety bands and service rules.

18. However, it must be emphasized that the entire concept and technical assumptions relate entirely to operation within the existing ISM bands, in which there is no protection given or received by definition. NPSTC is opposed in general to any extension of the concept to non-ISM bands, such as suggested for devices operating under §15.209 at low power levels in almost any frequency band (less TV bands and certain restricted bands). Such an arbitrary and unfounded extension of the proposal, without considerable study, could easily result in unforeseen problems and incompatibilities, possibly to public safety operations sharing with other services. Although not permitted under §15.209, NPSTC is opposed to any sharing of TV channels 14-20 beyond the current sharing with PLMR (Part 90) eligibles (that include many public safety users), in major metropolitan areas; NPSTC believes that it would be virtually impossible to keep such “sharing devices” from migrating around the country and into these major metropolitan markets where they would interfere with incumbent public safety users. NPSTC notes the proposed permanent sharing of TV channel 16 in the New York City metropolitan area for public safety operations as an example of the complex and sometimes critical sharing arrangements in many licensed bands.

V. SECONDARY MARKETS

19. NPSTC notes with considerable interest the extensive treatment (over 20% of the discussion) of the secondary markets issue, with emphasis on cognitive radio and interruptible spectrum leasing as the means to "address the issue of technical requirements for possible leasing

of public safety spectrum." It is the intention of the public safety sector to continue to consider the critical policy aspects of the issue in the context of the Secondary Markets FNPRM. NPSTC believes that the Commission is making two questionable assumptions on this issue: (a) that public safety has excess spectrum to lease, noting that with the recent allocation of 50 MHz in the 4.9 GHz band and the current unavailability of the 700 MHz band in much of the U.S. the local/state public safety community is still 47 MHz short of the 97 MHz of spectrum identified as a critical public safety requirement in the PSWAC Report, and (b) that other users would be willing to lease spectrum when it might be unavailable for days or weeks due to a major incident such as the wildland fires that routinely occur in the Western States.

Access/Reversion Mechanisms

20. The Commission has identified the speed with which a public safety licensee can reclaim access to its spectrum as an important consideration in any appropriate mechanism. As part of the *Statement of Requirements* described in the following section of these Comments, NPSTC notes that there is a quality of service performance requirement identified that establishes 250 milliseconds as the maximum call setup time for voice communications. This requirement is based upon current performance in virtually all small-to-large public safety networks, including those using simulcast transmitters, voting receivers, continuous tone-coded subaudible squelch, and multi-channel analog and digital trunking. Within this 250 ms period, the secondary market user would have to detect the presence of a public safety user and relinquish the spectrum while still allowing sufficient time for the public safety user to complete a number of network and device set-up functions. Thus, it is clear that the "reversion time" is significantly less than the 250 ms period.

21. The Commission requests comment on “beacon systems” used for sharing (NPRM at ¶57 and ¶62). This concept assumes that the public safety system user would want to broadcast its presence in an area, which is often not the case and even operationally unacceptable in certain situations. Public safety systems using simplex operation would require each subscriber set, already severely taxed by battery limitation to work for up to 12 hour shifts based upon a typical 5-10% transmitter cycle, to transmit a beacon signal during the other 90-95% of its duty cycle, simply an impossibility. Furthermore, a beaconing system capable of meeting the 250 ms reversion time would virtually mandate that full-duplex radios be used by both the public safety user and the sharing system to enable immediate access by each; each public safety subscriber would have to randomly listen through its beacon for other public safety transmissions, while the sharing user would have to likewise listen for the public safety beacon. If the security and anti-spoofing features discussed by the Commission (NPRM at ¶60) were to be implemented on any type of public safety system within this same reversion time limit, it would require a high very speed beacon signal, subject to all of the RF propagation limitations experienced in most spectrum (fading, multi-path, etc), along with potentially significant processing power within the receiving devices.

22. The Commission discusses a tiering system for public safety users (NPRM at ¶64), assuming that “instantaneous reversion may be unnecessary.” NPSTC notes that, particularly within the first responder community (emergency medical, fire and law enforcement), incidents that begin as “routine” can instantly change to “crisis” completely changing the nature of associated communications. Thus, attempting to identify less critical incidents and tier them to permit sharing is a non-starter for first responders.

VI. OTHER APPLICATIONS OF COGNITIVE RADIO

Facilitating Interoperability

23. The Commission's special focus on public safety interoperability (beginning at ¶74), while appreciated, demonstrates a clear lack of understanding within the FCC (and for that matter, in other governmental and industry circles) of the public safety community's day-to-day operation and its inseparable relationship to effective response and coordination in major disasters. To address this gap, the responsible agencies and public safety groups undertook during the past year to develop a definitive *Public Safety Communications and Interoperability Statement of Requirements*.⁵ The effort focused on operational and functional requirements, and is not based on any particular approach or technology.

24. It is anticipated that the document, jointly released by the U.S. Department of Homeland Security and U.S. Department of Justice on April 26, 2004, will provide important information to users, planners, industry, and many others regarding the baseline public safety needs, as well as insight to the possible role of advanced technologies such as SDR, cognitive radio, mesh networks, and the like. NPSTC will undertake to ensure the interested FCC staff is adequately briefed on the document.

Dynamically Coordinated Spectrum Sharing

25. The Commission is correct in its view that the inherent real-time awareness of cognitive radio devices appears well suited to assist in frequency coordination, more intense spectrum sharing and improved spectrum efficiency. Hence, application of this capability is likely to have a positive effect on spectrum usage and access, and the Commission is urged to move forward in

⁵ The SoR is on the Internet at http://safecomprogram.gov/files/PSCI_Statement_of_Requirements_v1_0.pdf

those bands and services where applicable and effective for the particular situation. In the public safety environment, the technique is not expected to be particularly relevant since infrastructure operates primarily in the one-to-many (multicast) mode, and good system design also incorporates “direct mode” or simplex unit-to-unit operation for the event of infrastructure failure, or for operations where there is no infrastructure coverage. On the other hand, there would appear to be potential benefit for disaster scene coordinators and similar large "mutual aid" situations, and therefore may be considered for the future.

Mesh Networks

26. NPSTC shares the Commission's assessment that mesh networks' ability to expand to areas beyond the reach of base stations can be useful to both licensed and unlicensed systems, to "self-heal" will offer benefits for improving reliability and to provide more spectrally efficient operation than conventional networks. As part of the *Statement of Requirements* described above in these Comments, there is a specific requirement that communications systems must be capable of supporting peer-to-peer applications and be self-healing. Hence, it is clear that advancements and deployment of mesh networks will be closely followed by the public safety sector and likely considered for deployment at the appropriate time in the future.

Frequency Selection for Unlicensed Devices

27. The Commission's objective to reduce the production and consumer costs of unlicensed devices by modifying Part 15 rules is appreciated and supported, provided the necessary safeguards are mandated and certified (such as through the "umbrella" approach described earlier in these Comments). Special attention will have to be given to an effective and assured

procedure to ensure that foreign devices brought into the U.S. do not operate on those channels not authorized for use by the FCC, such as in the case of the 4.9 GHz band and unlicensed U-NII type devices manufactured in Japan.

VI. EQUIPMENT AUTHORIZATION MATTERS

Submission of Radio Software

28. The original SDR proceeding adopted a requirement for the applicant to submit a copy, when and if requested by the FCC, of the software and source code that controls the RF configuration and changes in the device. NPSTC accepts the Commission's view that the software programs and code are too complex and variable, and therefore unlikely to assist FCC in determining whether unauthorized changes have or could be made to an SDR device. The proposed changes are reasonable and should be adopted.

Mandatory Declaration of SDR Devices

29. The Commission has advised that since adoption of the SDR rules, there have been no devices declared as an SDR, even though the FCC has, for many years, certified devices that clearly fit the definition. Such devices include many cellular handsets and indeed a number of PLMR radios used by the public safety community. The FCC then repeats its concerns about the potential threat to other spectrum users for the unauthorized use of software, and emphasizes that a manufacturer is not required to provide security features if it does not declare the device as an

SDR. NPSTC strongly urges the Commission to revise its approach, which appears to assume that security can only occur if the device is called an SDR.

30. The problem is not whether the device is an SDR or not, but rather, the concern and challenge is whether any device capable of remotely modifying RF parameters via software after manufacture is provided with adequate security to prevent unauthorized changes, to prevent the use of unapproved software, and to protect against interference, be it accidental, malicious, malfunction or other cause. Assuming security concerns can be handled effectively (as suggested elsewhere in these Comments), there is no apparent or obvious reason to change to a "mandatory declaration" for SDR. In addition, it is likely manufacturers will voluntarily declare SDRs as more come to market and benefits of streamlined software approval procedures are better understood.

Other Considerations Relating to SDR

31. The original SDR proceeding allowed a manufacturer to display a device's FCC identification number electronically, rather than on a physical label. In addition, the new rules did not require manufacturers to place a new identification number on a device if they choose to follow the streamlined filing procedure. In any event, the hard physical label could quickly become irrelevant and non-informative about the RF characteristics of the device, once it was modified by software. There appears to be no way for enforcement officials in the field to ascertain the actual RF configuration, since records only indicate what combinations may have been tested, but not the actual situation. The potential problem will expand as more SDRs and cognitive radios are deployed. Given the imminent shift to software-based devices, the

Commission is urged to mandate an "electronic label" as a replacement for the physical label. Various implications and options were provided in the SDR proceeding.

32. The original SDR proceeding also identified the potential benefits associated with third party software, such as innovation and competitive pricing. The issue is still timely and the benefits potentially greater, provided the security and safeguard issues can be satisfactorily addressed. Further, this matter is analogous to several of the specific proposals contained in the present NPRM, in that it is likely to lead to appreciable cost savings for the user and consumer over time. NPSTC urges the Commission to reopen this issue with a view to determining whether there are any new ideas or developments, and to identifying incentives for third party vendors and/or device manufacturers.

Applicability to Other Devices

33. As discussed above, it is inconsequential whether the device is an SDR, transmitter module, amateur radio equipment, computer technology, or whatever, provided the concerns regarding safeguards and security are effectively handled. NPSTC has proposed an alternative "umbrella approach" that would cover all the security concerns and questions raised by the Commission. Regarding the transmitter module, it would appear logical to treat it according to the basis device, e.g., SDR or non-SDR, and whether it can be remotely programmed or not. Regarding the amateur radio matter, NPSTC is opposed to a "hardware solution" as proposed in the NPRM, in the belief that the most effective solution is one that uses an appropriate mix of hardware, firmware, software, "trusted computing", physical security, and other measures for the given service and situation.

VII. PRE-CERTIFICATION TESTING REQUIREMENTS

34. The testing of radio devices for compliance and conformity as a pre-condition for certification under the FCC Regulations is a critical element of an effective spectrum management regime. In most cases, it is preferable that the tests be carried out by an approved Telecommunication Certification Body (TCB), as detailed earlier in these Comments.

Essential to Test Various Inputs and Combinations

35. The Commission is correct in its view that the customary testing of existing devices and services, generally involving a single or limited number of input conditions, is not sufficient for the highly flexible radios of the future. Cognitive radios, for example, may contain several capabilities in one device, such as the ability to change frequency, adjust output power, and modify its waveform, which are then selected according to some preset rules and policies based on the operating environment. Thus, it appears necessary to test the device over the full range of possible options and to validate results in response to various inputs or combination of inputs. As in the case of SDRs where testing included all combinations of hardware and software, cognitive radio testing should include all combinations of sensing, adapting and transmitting for all predictable situations, for both licensed and unlicensed devices.

Testing and Security Conformance a Vital Element of Public Spectrum Policy

36. As technologies like cognitive radio are introduced and spectrum policy provides for increased access through more efficiency and sharing, it is expected that there will be increased tension among spectrum users. On the one hand, new techniques needed for intensive and efficient spectrum use and promising substantial future benefits must move forward as quickly as

reasonable. On the other, existing users require protection from interference and other unacceptable disruption of long-standing operations, and must be given a demonstrated level of protection. In addition, there is a need for security conformity and other broad testing relating to software-based devices. NPSTC believes that adoption of effective pre-certification testing of cognitive radio and similar devices can provide a critical and essential balance between aggressive accommodation of new and innovative technologies and applications, and aggressive protection of existing users, systems and services, by demonstrating and proving the reliability and built-in safeguards of the proposed concept.

Proposed General Testing Framework for the Future

37. Such testing could become a valuable component of future public spectrum and technology policy. NPSTC urges the Commission to pursue establishment of a general framework for testing cognitive and similar future radios (while adopting specific procedures on a case-by-case basis in the near-term) based on the following principles:

- A. Pre-certification testing requirements should be developed and adopted for all CR and similar technologies in all situations involving a potential risk of interference to existing and/or new services.
- B. It should be assumed that FCC can not determine in advance all of the relevant functions, conditions, tests, etc. to allow adoption of universal rules for testing; hence, a structured process should be established to rapidly, yet effectively handle issues and questions as they arise.
- C. The process should determine the issues of concern, functions/conditions to be studied, and the tests to be conducted.
- D. The process should include or provide for:
 - 1) All interested parties, and in particular, sponsor(s) of the new technology/application and any potentially affected spectrum users.

- 2) Open access and participation, taking due account of proprietary information, and widely available results.
 - 3) Mandate for timely and expeditious progress of the activity, with due regard to the legitimate needs and concerns of all players.
- E. The process should be focused in and developed through an appropriate industry group (including a standards organization, if so indicated), with the FCC providing policy leadership, support and cooperation

38. With respect to pre-certification testing, the proposed process and its envisioned goals, it is noted that various organizations, such as NPSTC and the Telecommunications Industry Association, often have relevant expertise and useful input relative to such pre-certification testing and should be included.

VIII. CONCLUSIONS

39. In closing, NPSTC wishes to commend the Commission on the broad and far-reaching proceeding it has launched under the label of cognitive radio. The document gives a vivid picture of the rapidly changing spectrum environment, with heavy emphasis on the role of advanced technology, more intense packing of traditional frequency bands, and innovative and promising new techniques that will provide spectrum access for an exploding wireless demand in all sectors.

40. The Commission is urged to give special attention to the following items:

- A. Consideration and adoption of an alternative approach to the inherent security concerns and threats associated with software-configurable radios, which would shift from the SDR device-centric rule to one that directly targets the risks and threats.

- B. Unique and vital features of the public safety community, and in particular, to the just-released *Public Safety Communications and Interoperability Statement of Requirements*.
- C. Need for clear definitions of key terms, including cognitive radio, so as to avoid confusion (e.g., learning or not) and ensure that necessary analysis and testing is both doable and repeatable.
- D. Consideration and development of a general testing framework for pre-certification with a view to providing, as an integral component of an effective national spectrum policy, the essential analysis and demonstration of the many advanced techniques and innovative sharing situations in the future

Respectfully submitted,

Marilyn B. Ward, Chair
National Public Safety Telecommunications Council

NPSTC Support Office
NLECTC – Rocky Mountain Region
2050 E Iliff Avenue
Denver, CO 80208
(800) 416-8086

May 3, 2004