HARRIS,
WILTSHIRE &
GRANNIS LLP

1200 EIGHTEENTH STREET, NW
WASHINGTON, DC 20036

TEL 202.730.1300 FAX 202.730.1301
WWW.HARRISWILTSHIRE.COM

ATTORNEYS AT LAW

September 11, 2002

By Hand Delivery

Ms. Marlene Dortch
Secretary
Federal Communications Commission
The Portals
445 12th Street, S.W.
Washington, D.C. 20554

Re: ET Docket 00-47, In re Authorization and Use of Software Defined Radio (SDR)

Dear Ms. Dortch:

In response to the Commission's request for continuing information from industry about advancements in SDR security,[1] we have enclosed the SDR Forum's Report on Issues and Activity in the Area of Security for Software Defined Radio.

As the Report explains, the SDR industry has make quick progress on security issues. This is because it has been able to draw on a wealth of technical work that had already been done to protect digital assets generally. This means that the technology needed to ensure the security of SDR equipment already exists and its effectiveness has been proven in other sensitive areas. Specifically, techniques for maintaining the integrity of wireless communications and for safely transmitting sensitive content over the Internet (such as credit-card numbers) appear to be readily modifiable for use by SDR-based systems. These include public key cryptography, virtual private networks, firewalls, biometric technologies, and the use of security algorithms.

Moreover, manufacturers continue to have strong market incentives to implement effective and reliable security safeguards. Equipment manufacturers and wireless system operators well know that any security breach will directly result in lost revenue, lost subscribers, and the possibility of FCC enforcement action. The SDR Forum is confident that the added cost of state-of-the-art security will be well below the added value of the additional security.

The SDR industry is now doing the additional work needed to adapt proven security techniques to software defined radio. The SDR Forum is working to encourage this effort. It is also acting as a clearinghouse for information about the security of RF reconfigurable systems, ensuring that

[1] *In re Authorization & Use of Software Defined Radios*, First Report & Order, 16 FCC Rcd 17373, 17383 (2001).

organizations familiar with wireless and information security bring their expertise to bear on SDR security issues. The SDR Forum has worked, and will continue to work, with the wireless industry and with standards organizations to improve the security of SDR equipment, and plans to publish a second, more comprehensive report on the subject next year.

Almost a year ago, this Commission chose not to adopt specific security and authentication requirements for SDR-based systems, noting that "they could hinder the development of the technology used to provide such security and could have the potential to be unduly burdensome on manufacturers."[2] The Commission's goal was to give SDR equipment manufacturers the "flexibility to develop innovative software defined transmitting equipment," while retaining sufficient oversight over the security of SDR equipment through the equipment authorization process.[3]

That judgment was wise when made, and continues to be so. As the Commission anticipated, SDR Forum members have made – and will continue to make – great progress toward ensuring the security of software defined radios. New regulation would not hasten this effort, and could well thwart it. As part of its going efforts, the SDR Forum will continue to report to the Commission regularly on SDR security developments.

Pursuant to section 1.1206 of the Commission's rules, this letter and the attached materials are being electronically filed in the above-captioned docket.

Respectfully submitted,

Scott Harris

Scott Blake Harris
Counsel to the SDR Forum

Enclosure

cc: Ed Thomas, Chief, Office of Engineering and Technology
Bruce Franca, Deputy Chief, Office of Engineering and Technology
Julie Knapp, Deputy Chief, Office of Engineering and Technology
Lisa Gaisford, Chief of Staff, Office of Engineering and Technology

---

[2] *Id.*
[3] *Id.*