



1300 Pennsylvania Ave. NW
Suite 250
Washington DC 20004
October 11, 2005

ELECTRONICALLY FILED

Julius Knapp
Deputy Chief
Office of Engineering and Technology
Federal Communication Commission
445 12th Street SW
Washington D.C. 20554

Re: **EX PARTE** in ET Docket No. 05-183, Remington Arms Company, For Waiver of Sections 15.245, 15.247(b) and 15.247(e) of the Rules and Regulations

Dear Mr. Knapp:

On October 3, 2005, counsel for Remington Arms, Inc. provided to Julius Knapp proposed language for staff to consider in crafting conditions that would allow Remington Arms, Inc. to market and sell a noncompliant analog device (the Remington "Eyeball") utilizing unlicensed spectrum in the 2.4 GHz band. That note, attached here, was the product of a conversation between Cisco Systems and Remington. Cisco is hopeful that our discussion with Remington has narrowed the issues for resolution.

As discussed in the communication conveying the proposed conditions, the agreed-upon language represents a partial agreement among the parties. First, although both Remington and Cisco could agree that there should be a limitation on who could purchase and use the device, the two parties could not agree on the specific language of the limitation. Second, Cisco sought a condition that would limit the operation of the device to its battery power source, a condition on which Remington could not agree. Finally, Cisco remains uncomfortable with an open-ended waiver that will allow an analog device to be manufactured for the band indefinitely. The purpose of this letter is to provide Cisco's perspective on the issues on which we could agree. A summary of our additional proposed conditions is presented in the concluding paragraph.

Background. As you are aware, this case concerns a petition for waiver filed by Remington, which seeks to certify a noncompliant analog device for the digital 2.4 GHz

band. The device consists of a briefcase-sized control box and a remote video device that sends a video picture to the control box for display. The video uplink from the remote device operates on 2.4 GHz frequencies used by unlicensed digital devices, including wireless local area networks (WLANs). Remington and Cisco agree that when the Remington device is active, WLANs will experience harmful interference. The parties have not agreed on the degree of harmful interference. Remington has stated that interference could occur up to a distance of about 60-100' when the device is on.¹ From Cisco's perspective, Remington has not provided a key data point that would allow a complete interference analysis² and Remington's advocacy on this issue has failed to reveal how the device will affect WLAN data throughput rates.

Nor is it clear how the device will affect the new 802.11g higher speed 54 megabit WLAN systems that are the leading product in the market today. Based on the limited information in the record, Cisco has previously provided an analysis of separation distance – at what geographic separation will a WLAN begin to experience slower data transmission rates when the Remington device is operational? Our analysis showed that the effects on the new 802.11g devices is likely greater than the Remington interference analysis reveals, with some affect on data rates beginning at distances from about a city block to several city blocks depending upon whether the WLAN is operating indoors, out-of-doors. We continue to be concerned that the impact of the device on 2.4 GHz WLANs and other devices in the band is not knowable from the current state of the record. This is especially troubling since public safety is itself using 2.4 GHz for public safety broadband communications today. In addition, the device could impact home users of 802.11 as well as commercial enterprises that make extensive use of 2.4 GHz 802.11 gear.

Eligible purchasers/users. Both parties agree that the Remington device should not be available for mass market purchase. Both parties also agree that the need for a waiver is premised upon use of the device in the service of law enforcement and homeland security. Both parties also agree that, with respect to any limitations on sales or marketing of the device imposed by the Commission, Remington will in good faith make best efforts to comply with those conditions. However, Cisco and Remington have different views on how the FCC should direct Remington to restrict its sales and marketing efforts.

Remington's position is that sales should be restricted to entities that are licensed under the Part 90 "public safety" pool, along with state-licensed security and investigative services. In Cisco's view, Remington's proposal is both overbroad and unrelated to the justification that is has provided in the record.

¹ Remington Ex Parte, July 5, 2005.

² For example, Cisco asked Remington to provide information about the bandwidth at -30dB. Information about power density of the transmission would also be needed to analyze interference.

“State-licensed” security and investigative services, as we understand Remington’s use of the term, refer to private companies whose employees are licensed for the purpose of carrying firearms. According to the U.S. Department of Labor, Bureau of Labor Statistics, there were nearly one million people employed as security guards in the United States as of May 2004.³ There is no information from the BLS on how many of those people are licensed to carry firearms, but the large number of employees suggests that there are likely thousands of security firms many of whom would be eligible to purchase Remington’s device. For example, the Maryland Investigators and Security Association lists approximately 80 company members on its web site.⁴ The Private Investigators Association of Virginia claims 300 members.⁵

Remington states that these private security and investigative companies should be able to purchase and use the Remington device.⁶ As a result, the device could be deployed by thousands of private firms and by hundreds of thousands of employees, and for purposes entirely unrelated to public safety. Given these numbers, the potential for disruption to devices in the 2.4 GHz band is significant, even assuming, arguendo, that the harmful interference created by Remington’s device is limited to compliant devices within a city block.

Perhaps more significant than the sheer volume of devices that might be deployed under Remington’s eligibility criteria, there is the important issue about how the device would be utilized by private security and investigative firms. On this issue, there is a complete mis-match between Remington’s purported justification for its waiver, and its proposal to sell to security or investigative companies whose employees carry firearms. Remington’s advocacy in support of its waiver request is grounded on law enforcement’s need to utilize the device in life and death situations:

- “The Eyeball R1 System reduces the danger to life while gathering information in small hazardous and confined areas, such as buildings, caves, tunnels and alleys, making it well-suited to counter-terrorism and law enforcement operations in urban, rural and wilderness areas.” Remington Petition at 1.
- “The Eyeball R1 will be used in situations of extreme stress where the full attention of the immediate area will likely be devoted to the law enforcement operation in progress.” Remington Petition at 2.
- “It is essential that the Commission treat this request with expedited consideration, considering the potential for lifesaving applications and the ability to effectively counter various terrorist activities, including hostage taking and minimizing destruction that might occur in other standoffs.” Remington Petition at 4.

³ http://www.bls.gov/oes/current/oes_33pr.htm

⁴ <http://www.misahq.com/index2.ivnu>

⁵ <http://investigativeprofessionals.com/member/associations/piava.htm>

⁶ Remington Reply Comments at 5-6.

- “The units will be used in situations in which it is hazardous for a public safety officer to directly observe a location. Such situations occur a few times a month in medium-sized jurisdictions. These are not devices that will be used 24/7 or on every street corner.” Remington Ex Parte, July 18, 2005 at 2.

While Cisco appreciates the important role that security firms play in protecting people and property, a security firm confronted with a “situation of extreme stress,” “terrorism,” or “hostage-taking” would do the same thing you or I would do – call 911. While the Commission might decide based on this record that there is a legitimate need for first responders, national defense and homeland security agencies to have access to this device, there is simply no reason to expand its availability to thousands of private firms.

Nor is it clear what these private firms would do with the device, and why its use is so critical that the Commission should allow widespread sale of an analog transmitter in this digital band. Remington states that security firms could use the device in perimeter security applications, such as checking underneath cars coming into a campus. This rationale suggests that the device would be used routinely, and not in the emergency situations that Remington portrayed in its waiver request.

Cisco believes that routine use by private security firms represents a much greater risk of disruption to WLAN operations at 2.4 GHz than occasional law enforcement emergency use. The FCC should deny Remington’s request that would allow security and private investigative firms to purchase and use the device. There is no compelling reason to place this device in the hands of thousands of firms and potentially hundreds of thousands of employees when its analog transmissions could slow or stop the use of the unlicensed band by compliant devices.⁷

In addition, Remington also seeks to be able to sell the device to the Part 90 public safety pool licensees. As the Commission is well aware, the “public safety pool” in Part 90 consists of a broad array of organizations that extend well beyond law enforcement. Licensees in this pool include hospitals, other medical services delivery personnel or institutions, physicians, schools of medicine, forest conservation activities, ambulance companies, persons with disabilities and if minors, their parents or guardians, persons who operate emergency radio networks, persons or organizations operating school buses, and beach patrols.⁸ Why any of these types of public safety licensees should need the device that Remington proposes to sell is not evident from the record in this case. As with the security and private investigative firms, above, there is no pressing

⁷ Cisco recognizes that law enforcement may occasionally have a need for more routine use of the Remington device. Cisco asked, and Remington agreed, that it would include in its operational manual and technical training information on how to coordinate with existing users of the band in an attempt to find a channel different than one used by WLANs in the vicinity. It is important that the FCC include this condition in any waiver grant.

⁸ Section 90.20 of the Commission’s rules, 47 C.F.R. §90.20.

need for them to employ the device in the services that they perform. Moreover, simply because someone meets the Part 90 criteria should not allow them access to a device that might be used as an amusement, but that would disrupt compliant users of the 2.4 GHz band.

In Cisco's view, if the Commission chooses to grant the waiver, sales and use of the device should be limited to law enforcement, defense, and homeland security agencies of government at the federal, state, and local levels. That is the result that is supported by Remington's advocacy on the record, and, more importantly, the only result where the Commission might reasonably determine a public benefit exists that outweighs the harm to users who comply with the band requirements, and manufactures who make compliant devices.

Battery power only. As described to Cisco, Remington's video system is designed to work on a battery with a life of about two hours. The device then needs to be recharged for further use. There also appears to be some finite limit on the number of times a battery can be recharged. Both of these design characteristics would seem to support the emergency law enforcement use that Remington outlined in its waiver petition. The two hour battery life is adequate to sustain the device in emergency situations. The need to recharge, and the finite limit on the number of times the device can be recharged, also helps ensure that law enforcement will use the device sparingly, and in real emergency situations.

Cisco requested that Remington agree to a condition advising users that the device is intended to be operated using its built-in rechargeable battery only. Remington, however, declined to agree to that condition. This suggests that Remington is not opposed to wiring its video system to a permanent power source. In Cisco's view, this result would be disastrous to users of compliant equipment in the band. An "always-on" analog video transmission system will constantly emit energy into the frequencies that it is using, stopping or slowing WLAN use or other unlicensed device use. This result effectively preempts the band for Remington's device.

In Cisco's view, if a waiver grant is desired, the Commission should require Remington to counsel purchasers of the device that its operation is intended for use with the built-in rechargeable battery, and that any other power source is unlawful.

Conclusion. Section 15.5(b) of the Commission's rules is clear: devices operating on unlicensed frequencies shall not cause, and must accept, interference. When Remington's analog video system is turned on, it emits signals in the band that will cause interference to compliant technology. An owner of a WLAN device would be forced to find an open frequency not being used by the Remington device, and not adjacent to it. This is difficult enough in a corporate network, where there will need to be a diagnosis of the cause of network degradation. For residential WLAN users, who are generally not conversant with technology, it presents a significant obstacle to the use and enjoyment of the compliant equipment that they have installed. The more that the Remington devices are sold and used, the increase in likelihood that WLANs will experience harmful

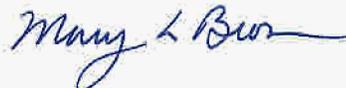
interference. While devices in this band are designed to accept interference from other digital transmissions, and to offer ways to work around that interference, at no time have devices in this band been asked to accept interference from analog transmissions.

A waiver of the digital requirements for the 2.4 GHz band to allow an analog transmitter to operate represents a significant change in policy, and a difficult challenge for the advanced technologies operating in the band today. If the Commission decides to grant this waiver on law enforcement's behalf, it should carefully consider how to narrow the scope of the waiver to produce the least harm to existing users, including consideration of a time limit on the waiver to encourage Remington to upgrade its technology to digital at the earliest practicable time. In Cisco's view, the Commission should consider a 24 month time limit on the waiver, which should be ample time for Remington to re-design the device in compliance with the rules for the 2.4 GHz band.

In summary, Cisco recommends the following conditions be placed on the grant of any waiver to Remington, in addition to those conditions previously presented by Remington (see attachment):

- Sales and use of the device should be limited to law enforcement, defense, and homeland security agencies of government at the federal, state, and local levels.
- Remington must counsel purchasers of the device that its operation is intended for use with the built-in rechargeable battery, and that any other power source is unlawful.
- Sunset the waiver at 24 months.

Sincerely,



Mary L. Brown
(202) 354-2923
marybrow@cisco.com

CC: Fred Campbell
John Branscome
John Giusti
Barry Ohlson