

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

---

*In the Matter of* )  
 )  
 )  
Remington Arms Company, Inc. Request for ) ET Docket No. 05-182  
Waiver of Part 15 )  
 )  

---

COMMENTS OF CISCO SYSTEMS, INC.

I. INTRODUCTION

Cisco Systems, Inc. (“Cisco”) hereby respectfully submits comments in response to the above-captioned Petition for Waiver.<sup>1</sup> Cisco is the worldwide leader in networking solutions for the Internet and is also a leading manufacturer of equipment for wireless services. Cisco offers a wide range of RF products that operate in “unlicensed”<sup>2</sup> frequency bands, and strongly supports spectrum-based solutions for broadband Internet access, and, more generally, wireless broadband. Cisco supports the important role the

---

<sup>1</sup> Public Notice, Office of Engineering and Technology Declares Remington Arms Company, Inc. Request for a Waiver of Part 15 To Be A “Permit-But-Disclose” Proceeding for *Ex Parte* Purposes, ET Docket No. 05-182, DA 05-1289, released May 5, 2005.

<sup>2</sup> As a legal matter, the use of the bands that do not require individual authorization is licensed by rule, rather than unlicensed. However, for sake of convention we will use the term “unlicensed” in this comment.

Commission has played in creating an environment that allows unlicensed bands to be widely shared, and that allows manufacturers to design and market advanced wireless devices in a reasonably cost-efficient manner.

Remington Arms Company, Inc. (“Remington”) has filed a petition for waiver of three sections of Part 15. Remington states that it has developed a short-range analog technology that allows video and audio surveillance of physical areas. Remington states that it expects that the analog surveillance device, known as the “Eyeball,” will be used by public safety organizations who may want to utilize the technology to monitor areas where it is undesirable to locate a human being. Among its other technical characteristics, the device will transmit audio and video to a control point using the 2.4 GHz unlicensed band. Remington is seeking a waiver of the transmit power limitation in Section 15.249(a) of the Commission’s rules so that it can exceed the power limit. In addition, because the device transmits using analog modulation, Remington seeks a waiver of 15.247(b)(3) of the Commission’s rules which would otherwise require digital modulation. As a corollary to this request, Remington also seeks a waiver of the spectrum density limits contained in Section 15.247(e) of the Commission’s rules. Remington states that if this were a digital device, no Section 15.247 waiver would be required.

Remington has not met its burden of demonstrating that a waiver is warranted in this case. Remington admits that the device will interfere with

other intentional transmitting devices operating in the band, including 2.4 GHz wireless local area networks (WLANs) used by police departments across the country. Remington has offered no evidence supporting its claim that its surveillance device will be restricted or limited to public safety uses in times of extreme emergency. In fact, Remington has not said that it will limit its marketing of the device and the technology only to public safety. Once the device is approved, Remington can sell the device to anyone, raising the prospect of widespread interference to existing devices. Moreover, Remington has not explained why it decided to create an analog device for unlicensed bands where digital transmissions are the norm, and where there exist other public safety bands where the device could be deployed. In public safety bands, law enforcement could manage spectrum use to avoid interference. A grant based on such an insufficient showing of good cause would potentially jeopardize future use of the band if other non-conforming technology is subsequently presented to the FCC for deployment at 2.4 GHz.

**II. DEPARTURE FROM EXISTING TECHNOLOGY NORMS FOR 2.4 GHz WILL DEGRADE THE UTILITY OF THE BAND FOR EXISTING USERS, INCLUDING PUBLIC SAFETY**

**A. Unlicensed bands today support public safety WLANs**

Remington, in its petition, argues that its proposed use of its analog surveillance technology by public safety merits grant of its waiver. Indeed, in its petition, the first three “reasons” it lists for why the waiver should be granted revolve around suggestions it has for how public safety might use the

technology. Significantly, Remington admits that if its technology is allowed to come to market, it will interfere with existing users in the band. The point that Remington completely misses is that some of those existing users are public safety departments themselves, which are increasingly deploying 2.4 GHz WLANs in support of voice, data, and video transmissions *in the field*.

As the Commission is well aware from its recent reconsideration of its decision in the 4.9 GHz docket, police departments around the country are deploying WLAN to support voice, data, and video communications in police vehicles. Mobile wireless routers are installed in the trunks of cars that can establish an 802.11 link to a control point. Some departments are installing control points at or near government facilities that permit secure mobile packet-based communications at data rates of 10-50 Mbps. Control points connect to the network using wireless bridges or fiber optic facilities. In some cases, public safety has achieved extensive geographic coverage of their communities. Below are a few examples of police departments that have adopted WLAN at 2.4 GHz to illustrate how the WLAN technology is being deployed from the largest cities to the smallest townships.

<b>Examples of Public Safety Organizations Deploying 802.11 Technology Today</b>	
<b>Los Angeles CA</b> (pop. 3.8m) PD: 27 WLANs at police stations throughout the city	<b>San Mateo CA</b> (pop. 92,500) PD: metro scale, WiFi mesh network
<b>Columbus OH</b> (pop. 711,500) PD: Linked city PD to surrounding PDs	<b>Buffalo Grove IL</b> (pop. 42,900) PD: Patrol cars and mobile incident command
<b>Baltimore MD</b> (pop. 651,200) PD: Initial deployment of 160 patrol	<b>North Miami Beach FL</b> (pop. 40,800) PD: metro area network

cars	
<b>New Orleans LA</b> (pop. 484,700) Police surveillance	<b>Upper Merrion Township NJ</b> (pop.30,000) PD: all patrol officers use the network, which covers 35% of the geography
<b>Aurora CO</b> (pop. 300,000) PD: mobile police and fire units	<b>Post Falls ID</b> (pop. 20,000) 23 access points with up to 5 mile radius; 22 patrol cars
<b>Syracuse and Onandoga County NY</b> (pop. 164,000) PD: 110 laptop equipped vehicles	<b>Isle MN</b> (pop. 700) 7-member police force equipped with 802.11b

In communities which have deployed 2.4 GHz systems in support of public safety, an officer sitting in his or her 802.11-equipped car and using a 802.11-equipped laptop can, among other things, file reports, access data, transmit video back to a command center, and have email functionality, as well. One interesting sidelight that Cisco has noted with its customer deployments, is that reliance on crowded analog voice channels drops in a significant way once a packet-based mode of communication is established.

While it is true that the Commission has recently revised its 4.9 GHz rules to permit WLAN technology to be deployed in licensed public safety spectrum at 4940-4990 MHz, the rule revisions were just published in the Federal Register on May 18, 2005.<sup>3</sup> As a result, equipment certification can only now begin. However, 2.4 GHz technology has been available to public safety for several years, and there is some “embedded base” of 2.4 GHz

---

<sup>3</sup> 70 Fed.Reg. 28463 (May 18, 2005). The new rules become effective July 18, 2005.

equipment. Those existing systems may well transition to 4.9 GHz, but the transition can be expected to take several years.

Of course, in addition to public safety users, there are millions of WLAN devices deployed in enterprises and households around the country. For example, the Commission's Wireless Broadband Task Force recently reported that 50 percent of enterprises use WLAN, there are more than 150,000 commercial hot spots, and between 2,500 – 8,000 Wireless Internet Service Providers.<sup>4</sup> WLAN has become an important technology for the delivery of wireless broadband service.

All of these devices, whether used in support of public safety, enterprises, or residential users, must accept interference and cannot cause interference to other users of the 2.4 GHz band.<sup>5</sup> What makes this band able to support such an important role in wireless broadband are both the Commission's technical rules limiting power and requiring digital transmission and, with WLAN deployed so ubiquitously in this band, the contention-based protocols on which WLAN technology is built.

**B. Absence of limitations on use or sales/marketing of Remington surveillance device means that use could be widespread and random**

Remington's petition makes a variety of observations about how its analog surveillance device might be used in support of public safety.

---

<sup>4</sup> "Connected and on the Go; Broadband Goes Wireless" Report by the Wireless Broadband Access Task Force, February 2005 at 30-32.

<sup>5</sup> 47 C.F.R. § 15.5(b).

However, these are just observations. Public safety organizations might deploy the device in response to extreme emergencies, or they might decide the device has greater utility and deploy it routinely. Acceptance by public safety of video monitoring as a public safety tool is well-known, with deployments that are as diverse as monitoring public spaces or for vehicular traffic control. One might easily imagine how a portable device could be used in support of routine investigations.

Moreover, the petition presents no information to suggest how or why this analog surveillance device would be limited to use by public safety. The device itself has not been designed or built to be used in a licensed public safety band. Instead, it is in an unlicensed band that can be used by anyone. Assuming that the device can or will be purchased by anyone, its widespread use could significantly degrade the operation of unlicensed intentional transmitters in the 2.4 GHz band, including WLAN, given that Remington asserts interference will occur up to an area the size of a city block.

### **III. WAIVER PETITION FAILS TO DEMONSTRATE SPECIAL CIRCUMSTANCES EXIST TO WARRANT GRANT**

The Commission's rules provide that no waiver can be granted unless the applicant makes a "good cause" showing to support the grant.<sup>6</sup> A waiver can be granted "...in specific cases only if [the Commission] determines, after careful consideration of all pertinent factors, that such a grant would serve the public

---

<sup>6</sup> 47 C.F.R. §1.3.

interest without undermining the policy which the rule in question is intended to serve.”<sup>7</sup> Thus, the applicant must both articulate how the public interest is served and articulate the special circumstances to prevent discriminatory application of the Commission’s waiver standard.

**A. Remington offers no showing about why 2.4 GHz is necessary or why other bands could not be used that Public Safety can actively manage**

Remington’s petition does not explain why it selected 2.4 GHz as the band over which it would transmit video and audio signals. The petition only explains that it will use 900 MHz frequencies for the downlink, while using 2.4 GHz for an uplink. Of course, there are licensed public safety frequencies scattered throughout the U.S. table of frequency allocations. These allocations either are, or can be, actively managed by public safety users. As a result, a public safety spectrum manager deploying a video surveillance technology could manage other communications around the need to establish a short-range video link such as one required by Remington’s device. Instead, however, Remington chose to develop its device to operate in the unlicensed band. At a minimum, Remington should explain why it is impossible or impractical to develop this technology for the licensed public safety bands.

---

<sup>7</sup> Petition for Waiver of the Part 15 UWB Regulations Filed by the Multi-band OFDM Alliance Special Interest Group, ET Docket No. 04-352, released March 11, 2005, *citing WAIT Radio v. FCC*, 418 F.2d 1153 (D.C. Cir. 1969); *Northeast Cellular Telephone Co. v. FCC*, 897 F.2d 1164 (D.C. Cir. 1990).

**B. There is no net benefit to support a public interest finding, and grant would undermine existing Commission policy**

Remington's request fails to meet the legal requirements for grant of a waiver. First, there are no special circumstances established by the request. Statements that the device will be used by public safety only in unusual situations and for limited time periods are simply descriptions of how the device might be used. Of even greater concern, Remington does not explain or commit to ensuring that devices are purchased and used by bona fide public safety organizations, especially since it is offering these devices in an unlicensed band. As a result, the only safe assumption is that these devices will become publicly available and widely used. Remington's arguments do not establish "special circumstances" supporting a waiver.

Moreover, the public interest is not furthered by grant of the waiver. Remington's admission that the device would cause interference to 2.4 GHz devices over areas up to and including an area the size of a city block would substantially devalue the utility of the band for unlicensed users operating in the band today. This is particularly true since it must be assumed that there will be no limitations on who might purchase and use the device. It is difficult to see how the public interest is furthered by grant of the Part 15 waivers when the result would be to devalue the substantial use of the band by existing users.

Finally, Remington argues that its analog surveillance device causes no more "interference" than digital devices using the band today.

The video transmission in the 2.4 GHz ISM will be at 1,000 rnW and will have a 6 dB bandwidth of approximately 2 MHz. Part 15.247(b)(3) permits digital transmissions at powers up to 1,000 mW in that same band provided that the 6 dB bandwidth of the

signal exceeds 500 kHz (47 CFR 15.247(a)(2)). The video transmissions from the Eyeball R1 can be expected to generate interference that is roughly comparable to such permitted digital devices. That is, the Eyeball R1 video transmissions can be expected to create approximately the same interference as devices currently permitted under the rules without waiver.<sup>8</sup>

But Remington's device causes substantially different interference than digital devices using the band today. The Remington device will simply occupy the frequency of its choosing, transmitting in analog and causing interference to other users. Unlike WLAN devices that predominate in the band, the device does not appear to employ cognitive radio techniques such as "listen before talk" or frequency hopping capabilities to avoid interference, as the WLAN devices do. Given how use of the 2.4 GHz band has evolved, its importance to public safety users, and its importance to the delivery of broadband wireless services to millions of enterprise and residential users, the Commission should not grant a Part 15 rule waiver that will permit introduction of a device that will degrade the operation of existing intentional transmitters operating in the band, and especially based on the thin argumentation provided by Remington.

#### **IV. CONCLUSION**

Based on the Petition for Waiver presented by Remington, Cisco recommends the Commission deny the above-captioned request for waiver of Part 15 of its rules. A grant based on such an insufficient showing of good cause would potentially jeopardize future

---

<sup>8</sup> Petition at 3.

use of the band, both with respect to the operation of Remington's device, and if other non-conforming technology is subsequently presented to the FCC for deployment at 2.4 GHz.

Respectfully submitted,

CISCO SYSTEMS, INC.

Mary L. Brown  
Senior Telecommunications  
Policy Counsel

1300 Pennsylvania Ave. NW  
Suite 250  
Washington, DC 20004  
202.354.2923  
[mary.brown@cisco.com](mailto:mary.brown@cisco.com)

June 6, 2005