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

In the Matter of	)	
	)	
Terrestrial Use of the 2473-2495 MHz Band for Low-Power Mobile Broadband Networks;	)	IB Docket No. 13-213
	)	
Amendments to Rules for the Ancillary Terrestrial Component of Mobile Satellite Service Systems	)	RM-11685
	)	

To: The Commission

COMMENTS OF THE
ALARM INDUSTRY COMMUNICATIONS COMMITTEE

The Alarm Industry Communications Committee ("AICC"), on behalf of its members,[1] hereby files its comments on the Notice of Proposed Rulemaking ("NPRM") in which the Commission proposes modified rules for the operation of the Ancillary Terrestrial Component ("ATC") of the single Mobile-Satellite Service ("MSS") system operating in the Big LEO S band, which would allow petitioner Globalstar, Inc. ("Globalstar") to provide low-power ATC using its licensed spectrum at 2483.5-2495 MHz, as well as spectrum in the adjacent 2473-

[1] Central Station Alarm Association (CSAA), Electronic Security Association (ESA), Security Industry Association (SIA), Bosch Security Systems, Digital Monitoring Products, Digital Security Control, Telular Corp, Honeywell Security, Vector Security, Inc., ADT LLC, AES-IntelliNet, Alarm.com, Bay Alarm, Intertek Testing, Security Network of America, United Central Control, AFA Protective Systems, Vivint (formerly APX Alarm), COPS Monitoring, DGA Security, Security Networks, Universal Atlantic Systems, Axis Communications, Interlogix, LogicMark, Napco Security, Alarm Detection, ASG Security, Security Networks, Select Security, Inovonics, Linear Corp., Numerex, Tyco Integrated Security, FM Approvals, the Underwriters Laboratories, CRN Wireless, LLC and Axesstel.

2483.5 MHz band.[2] As discussed in greater detail herein, AICC is concerned that Globalstar's operations in the 2473-2483.5 MHz band could inadvertently hinder public safety response to emergency situations by causing interference to critical alarm signals sent with the assistance of Wi-Fi equipment commonly operating on spectrum immediately adjacent to that band.

AICC member companies protect over 30 million residential, business and sensitive facilities and their occupants from fire, burglaries, sabotage and other emergencies. Protected facilities include government offices, power plants, hospitals, dam and water authorities, pharmaceutical plants, chemical plants, banks, schools and universities. In addition to these commercial and governmental applications, alarm companies protect a large and increasing number of residences and their occupants from fire, intruders, and carbon monoxide poisoning. Alarm companies also provide personal emergency response service (PERS) that allows consumers to summon help in the event of medical or other emergencies.

With the availability of more effective encryption technologies, a growing number of alarm systems include Wi-Fi connectivity in the alarm panel. Wi-Fi offers many benefits to both the alarm company and the customer: It is relatively straight-forward to install, obviates many of the service and installation issues associated with the point-of-entry in the home, and is increasingly already installed in the home or business of the customer.

Alarm companies rely on a variety of communications technologies to relay alarm signals to the central station quickly and reliably, including traditional telephone service ("POTS"), Voice over Internet Protocol ("VoIP"), cellular service, and dedicated central station alarm

[2] *In the Matter of Terrestrial Use of the 2473-2495 MHz Band for Low-Power Mobile Broadband Networks; Amendments to Rules for the Ancillary Terrestrial Component of Mobile Satellite Service Systems*, Notice of Proposed Rulemaking, FCC 13-147, IB Docket No. 13-213, RM-11685, released November 1, 2013.

frequencies. In addition, alarm technologies must connect the various components of the system (such as window and door contacts, smoke detectors, carbon monoxide detectors, and cameras) to the alarm panel at the protected premises. Increasingly, alarm systems are able to take advantage of WiFi technology to accomplish this connection, by incorporating WiFi-enabled sensors in alarm devices.

In addition, customers often require multiple paths for alarm signals, to ensure that each signal concerning a fire, home invasion or medical emergency is received even if, e.g., telephone lines are damaged. Certain alarm technologies are incorporating access to the internet, including WiFi connections, as a way to accomplish an affordable alternative path to the central station.

Creating such affordable alternative is likely to become very important in the near future: The most prevalent of alarm transmission technologies, POTS, is in the process of being retired by the large telecommunications carriers at a breakneck pace. The FCC has begun the process of reviewing and authorizing TDM-to-IP transition trials.[3] Many states, often at the behest of AT&T, are passing or considering passing legislation that would reduce or outright eliminate restrictions on retiring POTS.[4] Cellular service, another widespread alarm signal transmission technology, is currently facing the retirement of 2G technology, which will require a monumental effort on the part of the alarm industry to ensure service is not disrupted during the required change-over to LTE or other 4G technology.[5]

---

[3] *In re: Technology Transitions, et. al,* FCC No. 14-5, GN Docket Nos. 13-5, 12-353; WC Docket Nos. 10-90, 13-97; CG Docket Nos. 10-51, 03-123, released January 31, 2014.
[4] *See, e.g.,* S.B. 99, 2014 Regular Session (KY 2014); S.B. 636, 97th Leg., Regular Session (MI 2014); H.B. 1608, 2013-2014 Regular Session (PA 2013).
[5] *See, e.g.,* Peter Svensson, AT&T Sets Deadline for 2G Sunset in 4 Years, USA Today, August 3, 2012 (available online at http://usatoday30.usatoday.com/tech/news/story/2012-08-03/att-2g-network/56758432/1, last visited May 1, 2014).

As AICC has demonstrated in other proceedings, VoIP has a host of issues plaguing its reliability. For example, many VoIP-based services do not support line seizure, an important alarm function that ensures signals are transmitted even while the line is in use; and where line seizure *is* possible, some providers do not take line seizure into account when installing broadband service and bypass the line seizure device, rendering it inoperable.[6] Moreover, not all VoIP services are able to appropriately encode and decode the tone messages sent by alarm panels.[7] Even where alarm signal transmission is correctly implemented, it has been the alarm industry's experience that frequent maintenance is a reality of VoIP service, and the software-based nature of the service creates the possibility of on-the-fly modifications to the service that may impact the ability of alarm signals to be transmitted without the customer's realization.

The alarm industry is not the only group coming to rely on WiFi as an integral part of their operations, as the Commission and industry sources note that businesses and consumers by the millions are utilizing WiFi as part of the explosion in wireless broadband use.[8] The Commission has therefore appropriately noted the concerns that have already arisen concerning the potential for interference from Globalstar's proposed system.[9] A number of commenters in the proceeding have indicated that Globalstar's proposal may have a substantial and negative impact on Wi-Fi operations in the relevant band. Both the Wi-Fi Alliance ("Alliance") and the Bluetooth Special Interest Group ("BSIG") raised interference concerns with Globalstar's proposal, specifically citing a potential loss in service due to loss of the guard band between

---

[6] *See, e.g., Reply Comments of the Alarm Industry Communications Committee*, GN Docket No. 13-5, filed August 7, 2013; *Reply Comments of the Alarm Industry Communications Committee*, GN Docket No. 09-191, 07-52, filed March 5, 2010.

[7] For wired services, the National Fire Protection Association (NFPA) created the Managed Facilities Voice Network standard in recognition of this problem, though few carriers follow it. *Alarm Industry Communications Committee Notice of Ex-parte*, GN Docket Nos. 13-5, 14-28, CC Docket Nos. 95-20, 98-10, filed April 4, 2014.

[8] NPRM at para. 13.

[9] NPRM at para. 16.

Globalstar's licensed spectrum and the adjacent unlicensed band.[10] The Consumer Electronics Association ("CEA") filed reply comments echoing those concerns, and adding yet others to the list.[11] The record in this proceeding reflects the concern that interference to the millions of existing WiFi devices already in use could force an unnecessary and extremely burdensome replacement process, which must be weighed against any benefits from Globalstar's operations.[12] With more and more WiFi devices being deployed in alarm operations, AICC shares this additional concern. The record also reflects the legitimate concern that Globalstar's proposal may put American WiFi and Bluetooth manufacturers at a disadvantage, given that the 2400-2483.5 MHz band has been globally harmonized for WiFi.[13] This disadvantage would likely translate into higher equipment costs for industry members and consumers alike, not to mention harm to the U.S. economy.

These concerns are heightened because of Globalstar's intent to ultimately utilize somewhat higher powered equipment in certain portions of its system.[14] As noted above, alarm companies and their customers are increasingly turning to Wi-Fi as an alarm signal transmission technology to complement the existing technologies; and as the Commission encourages the transition of telecommunications and carriers to IP-based and wireless technologies, it is important that alarm systems be able to make this transition. Therefore, the Commission must do everything possible to ensure that nothing interferes with Wi-Fi service. This includes ensuring that any operations by Globalstar do not interfere with the efficient utilization of WiFi under the

---

[10] *See* Comments of the Wi-Fi Alliance, RM-11685 (filed Jan. 14, 2013) ("Alliance Comments"); Comments of the Bluetooth Special Interest Group, RM-11685 (filed Jan. 14, 2013) ("BSIG Comments").
[11] *See* Reply Comments of the Consumer Electronics Association, RM-11685, (filed Jan. 29, 2013).
[12] *See* January 14, 2013 Comments of WISPA at p. 4.
[13] *See* Alliance Comments at p. 5.
[14] *See, e.g., Petition of Globalstar, Inc. for Rulemaking to Reform the Commission's Regulatory Framework for Terrestrial Use of the Big LEO MSS Band*, RM-11685 (filed Nov. 13, 2012)(Globalstar Petition) at pp. 40-41; NPRM at para. 29.

current rules that require all users to obey protocols designed to avoid disruption of other users. The NPRM appears to indicate that the Commission shares this goal.[15] Before a determination can be made that Globalstar's proposed system can go forward, thorough testing must be conducted by a truly independent testing authority, utilizing a significant and diverse test bed. It is respectfully submitted that testing conducted by Globalstar or its contractors is not sufficient, given the obvious room for biased results. Affected stakeholders (including WiFi manufacturers, WISP providers, Bluetooth manufacturers, alarm industry representatives, and consumer advocates) should be allowed to participate in the testing process.

AICC also supports the Commission's proposal that Globalstar not be granted any additional interference protection rights in the unlicensed bands, but instead be subject to the same rules that apply to other unlicensed users. *See* NPRM at paras. 19-20. However, AICC remains concerned about the concerns raised by other parties that the loss of the de facto guardband for WiFi may have a cascading effect, reducing the amount of spectrum available in an already crowded spectrum environment.

Finally, AICC appreciates Globalstar's recognition of the importance of protecting GPS communications. See Globalstar Petition at p. 45. While Globalstar indicates its believe that its proposed operations in the Lower Big LEO band "are unlikely to cause harmful interference to GPS receivers",[16] it is respectfully submitted that protection of GPS must be confirmed and mandated. Alarm companies, like so many other businesses and individuals, depend on the

[15] *See* NPRM at para. 16 ("We believe that Globalstar's proposal to deploy a low-power terrestrial system in the 2473—495 MHz band should be examined to determine whether it is possible to increase the use of this band and adjacent bands, *without causing harmful interference to users of this band and adjacent bands*, . . .") [Emphasis added]
[16] *Id.*

reliability of GPS for various tracking and security functions, as documented in AICC's comments in other proceedings.[17]

Respectfully submitted,

Alarm Industry Communications Committee

By: /s/ John A. Prendergast
John A. Prendergast
Salvatore Taillefer, Jr.
Its Attorneys

Blooston, Mordkofsky, Dickens,
Duffy, & Prendergast, LLP
2120 L Street NW
Suite 300
Washington DC 20037
Tel: 202-659-0830

Dated: May 5, 2014

[17] *See* March 1, 2012 Comments of AICC in IB Docket No. 11-109 (*In Re LightSquared Subsidiary LLC*).