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

In re	)	
	)	
Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan; National Broadband Plan Public Notice #8	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	PS Docket Nos. 06-229, 07-100, 07-114
	)	WT Docket No. 06-150
	)	CC Docket No. 94-102
	)	WC Docket No. 05-196
	)	

COMMENTS OF CTIA—THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Brian Josef
Director, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Dated: November 12, 2009

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY 1

II. THE COMMISSION SHOULD ENSURE THAT ANY REQUIREMENTS FOR NEXT GENERATION 911 SERVICES MUST BE TECHNOLOGY NEUTRAL AND TECHNICALLY FEASIBLE 2

III. CYBER SECURITY IS A GROWING ISSUE THAT HIGHLIGHTS THE NEED FOR REASONABLE NETWORK MANAGEMENT OF WIRELESS SYSTEMS 9

IV. THE COMMISSION AND OTHER FEDERAL AGENCIES SHOULD REMAIN FOCUSED ON THE COMPLETION OF SPECIFICATIONS FOR COMMERCIAL MOBILE ALERT SERVICES 13

V. CONCLUSION 16

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

In re	)	
	)	
Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan; National Broadband Plan Public Notice #8	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	PS Docket Nos. 06-229, 07-100, 07-114
	)	WT Docket No. 06-150
	)	CC Docket No. 94-102
	)	WC Docket No. 05-196
	)	

COMMENTS OF CTIA—THE WIRELESS ASSOCIATION®

I. INTRODUCTION AND SUMMARY

CTIA—The Wireless Association® ("CTIA")[1] hereby submits its comments in response to the Federal Communications Commission's ("FCC" or "Commission") National Broadband Plan ("NBP") Public Notice #8 ("Public Notice") seeking comment on broadband issues related to certain public safety, homeland security, and cyber security initiatives.[2] In response to the Commission's inquiries about the development of Next Generation 911 ("NG911") systems, CTIA urges the Commission to engage in a technology neutral and consensus-driven approach that will involve all stakeholders. Also, CTIA reminds the Commission that significant funding challenges exist for public safety answering points ("PSAPs") that are currently slowing the deployment of E911 and must be resolved to ensure a successful NG911 build-out. Regarding cyber security, CTIA details some of the dynamic means of network management that wireless

[1] CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, Advanced Wireless Service, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[2] Public Notice, "Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan, NBP Public Notice #8," GN Docket Nos. 09-47, 09-51, and 09-137, PS Docket Nos. 06-229, 07-100, and 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196, DA 09-2133 (rel. Sept. 28, 2009) ("*Public Notice*").

carriers utilize to protect their subscribers from cyber attacks. CTIA stresses that network operators require significant flexibility in their network management approaches to respond to the ever-changing nature of cyber threats. Finally, with respect to emergency alerting systems, CTIA discusses the ongoing development of the Commercial Mobile Alert System ("CMAS") protocols and the important steps that have yet to be taken to enable initial deployments of this service. CTIA cautions that the first generation of CMAS should be tested, developed and deployed before any new broadband-based functionalities are demanded of CMAS and that last minute efforts by broadcast radio entities to mandate their particular technology for CMAS are misguided, inappropriate and already were considered at length by the Commercial Mobile Service Alerts Advisory Committee ("CMSAAC") and ultimately dismissed.

II. THE COMMISSION SHOULD ENSURE THAT ANY REQUIREMENTS FOR NEXT GENERATION 911 SERVICES MUST BE TECHNOLOGY NEUTRAL AND TECHNICALLY FEASIBLE

The *Public Notice* seeks comment on the development of systems and practices designed to enable the public to use broadband technologies to better communicate with emergency responders.[3] When fully developed, NG911 systems will enable PSAPs to receive and transmit various kinds of electronic information between civilians, first responders, law enforcement personnel, and others. The National Emergency Number Association ("NENA"), which is coordinating one NG911 standards-development project, indicates that in addition to voice calls, a NG911 system will allow PSAPs to handle numerous different types of communications, including data, images, video, and telematics.[4] Further, NENA envisions NG911 systems providing PSAPs the ability to supply first responders with information such as building plans

[3] *See Public Notice* at 2.

[4] *See* NENA, "What is NG9-1-1?" *available at* http://www.nena.org/sites/default/files/NG9-1-1%20Definition%20Final%201.1.pdf (last visited Nov. 8, 2009).

and patient medical files, all while enabling coordination between jurisdictions and across borders.[5]

In examining NG911, CTIA urges a process involving all stakeholders – including wireless carriers and manufacturers, public safety entities, transportation authorities, and others – similar to the one used to develop the rules governing wireless emergency alerts. CTIA has suggested in the past the formation of an E911 working group resembling the CMSAAC, established under Section 603 of the Warning, Alert and Response Network Act ("WARN Act").[6] CTIA believes that this type of cross-industry and government forum represents a prudent means of addressing NG911 issues, capabilities and solutions. This process also should incorporate input from consumers, specifically including individuals with disabilities, who potentially stand to benefit from increased accessibility to NG911 services. CTIA and the wireless industry welcome the opportunity to meet the unique needs of the disability community as wireless devices and services have become important to their safety and security, whether asking for help or receiving critical information during an emergency.[7] A collaborative approach will ensure that the regulatory requirements adopted by the Commission are both technology neutral and technically feasible – leading to the full benefits of technology being rapidly and effectively deployed to the American public. Any failure to include all interested

---

[5] *See id.*

[6] *See, e.g.*, CTIA Comments, E911 Location Accuracy Requirements, PS Docket No. 07-114, *et al*. at 2 (Aug. 20, 2007).

[7] According to a recent survey, individuals with disabilities place significant importance on wireless devices and services for communications during an emergency. Rehabilitation Engineering Research Center for Wireless Technologies, Second Report: Findings of the Survey of User Needs (SUN) for Wireless Technology 2007-2009, 5 (March 2009) ("Wireless RERC SUN"). *See also* Intelligent Transportation Systems, U.S. Dept. of Transportation, *Next Generation 9-1-1 (NG 9-1-1) System Initiative: Proof of Concept Testing Report* (Sept. 17, 2008) ("DOT NG9-1-1 Proof of Concept Report") (finding that migration to IP-enabled 9-1-1 systems in general represents the critical path for meeting the needs of people with disabilities) *available at* http://www.usatoday.com/tech/wireless/2009-08-10-911text_N.htm

parties will prolong the compliance process and lead to inefficiencies and ineffectiveness of these important programs.

Additionally, this process should be conducted in collaboration with other Federal and state regulatory agencies with an interest and experience in NG911, including the NTIA National E911 Implementation Coordination Office.[8] One such agency that the Commission should continue to work with is the Department of Transportation, whose own NG911 initiative has already led to a five-city proof-of-concept test demonstrating the operation of an IP-based PSAP with functionalities including caller location identification and transmitting and receiving text messages and vehicle telematics data.[9]

The *Public Notice* asks about the broadband infrastructure required to support NG911 deployment,[10] however, trials of NG911 systems have only just begun. For example, as recently as August, 2009, Black Hawk County, Iowa became the first U.S. jurisdiction to enable its 911 systems to accept text messages.[11] The Black Hawk County system claims to allow citizens to contact 911 via short message service ("SMS") text message, which could be useful to the hearing-impaired. Only customers of one local wireless provider, however, have access to the new service.[12] Although similar trials and deployments may be planned or ongoing elsewhere, the technical and operational specifications of a true NG911 system are not yet finalized. As such, Commission inquiries as to the broadband infrastructure requirements necessary to support NG911 capabilities are likely premature.

---

[8] *See, e.g.,* http://www.e-911ico.gov/NationalNG911MigrationPlan_sept2009.pdf (last visited Nov. 10, 2009).

[9] *See* Intelligent Transportation Systems, U.S. Dept. of Transportation, *Next Generation 9-1-1 (NG 9-1-1) System Initiative: Proof of Concept Testing Report* (Sept. 17, 2008) *available at* http://www.usatoday.com/tech/wireless/2009-08-10-911text_N.htm ("DOT NG9-1-1 Proof of Concept Report").

[10] *Public Notice* at 2.

[11] *See* Grant Shulte, *:(help! asap: Iowans Put 911 Texting To Test*, USA Today, Aug. 10, 2009 *available at* http://www.usatoday.com/tech/wireless/2009-08-10-911text_N.htm.

[12] *Id.* CTIA notes that this trial may have benefited from being more inclusive of the wireless industry as part of its rollout and that it should not be looked at as a model for national 911 text messaging.

Groups such as the Association of Public-Safety Communications Officers ("APCO"),[13] NENA,[14] and the Internet Engineering Task Force ("IETF") have developed standards to address the provision of location information and other operational considerations necessary to support voice over Internet Protocol ("VoIP") 911 calling. However, work still remains to ensure that such efforts are fully compatible with next generation wireless air interfaces, and to finalize the detailed specifications of a fully IP-based emergency services infrastructure network.[15]

In general, new packet-based wireless technologies are nascent, and are still undergoing widespread deployment. In light of the ongoing technological development, both on the wireless broadband access side, and from the perspective of the public safety community, the Commission must take care not to regulate new wireless technologies without a full appreciation of the effects of such regulation. Thus, as noted above, a consensus-based approach that leads to reasonable and effective regulation is most appropriate for any action the Commission may take with respect to NG911.

As the Commission is aware, one challenge of providing emergency services today is the acquisition of accurate location information for VoIP and wireless 911 callers. As NG911 deploys, and the public is able to request emergency services using additional means of digital communication, this challenge has the potential to escalate. It is likely that the vast majority of next generation wireless devices will be location-enabled – primarily through the use of embedded GPS chips. Standards development efforts are presently under way to ensure that accurate location information generated by wireless devices is capable of being received and

---

[13] *See* APCO, "APCO Project 41 (LOCATE-VoIP)", http://www.apcoproject41.org/ (last visited Nov. 9, 2009).

[14] *See* NENA, "Interim VoIP Architecture (i2)", http://www.nena.org/standards/technical/voip/interim-voip-architecture-i2 (last visited Nov. 9, 2009).

[15] *See, e.g.*, NENA, "NG9-1-1 Project: Overall NG9-1-1 Status", http://www.nena.org/ng911-project/overall-ng911-status (indicating that NENA estimate that "the earliest a tested, fully featured and standards compliant NG9-1-1 system could be realized is the end of 2010) (last visited Nov. 9, 2009).

used by NG911-enabled PSAPs.[16] It is undeniable, however, that the rapid pace of change in the constantly innovating and evolving wireless ecosystem underscores the need to take time at the outset of the process to develop resilient, effective industry standards and determine how best to coordinate the various pieces before mandating deployment. As Dale Hatfield observed:

> Even though the overall deployment of VoIP has been slower than many observers initially foresaw, the trend is clear and the implications for emergency services are significant. Clearly, the long term network architecture and other issues associated with the movement towards VoIP could be addressed by the Advisory Committee or other entity with overall system engineering responsibilities …. As I envision it, that entity would work with the Commission and the various wireless, wireline, and Internet standards groups to facilitate the necessary exchange of information to reach the necessary consensus to ensure a seamless E911 system in an increasingly IP-oriented national infrastructure.[17]

Wireless carriers alone annually collect nearly $2 billion dollars of dedicated taxes, fees and surcharges from wireless consumers for the purpose of supporting and upgrading the capabilities of the 6,174 Public Safety Answering Points (PSAPs) that exist across the country. In addition to the nearly $2 billion dollars annually collected from consumers and remitted to state and local governments, wireless service providers also have expended billions to modify their networks to enable them to identify and locate wireless E911 callers. Despite the billions being invested by wireless carriers to enable E911 and NG911 functionality, the public will not be able to enjoy the increased safety benefits of these systems without a substantial investment by public safety entities.

CTIA notes that one of the "lessons learned" from wireless E911 is that it is both inefficient and detrimental to require carriers to deploy new 911 technologies before PSAPs are able to utilize them. It is inefficient because it needlessly causes providers to incur costs with no

---

[16] *See, e.g.*, http://www.nena.org/sites/default/files/08-002%20V1%2020071218.pdf (last visited Nov. 11, 2009).

[17] Dale N. Hatfield, A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Services, at § 4.4, p. 42 (Oct. 15, 2002).

benefits, and it is detrimental because forcing the earliest possible deployment of new technology locks in the technology – and thanks to Moore's law and its corollaries, over time GPS and other location-based services become more accurate, faster in ascertaining the location, and less expensive. Thus, mandating carrier deployment before PSAP readiness has the strong probability of resulting in a more expensive yet less accurate solution.

PSAPs need to ensure that their networks are upgraded to match the technology developments of wireless providers, and to support the IP-based operations of NG911.[18] This represents a major challenge, as a number of PSAPs have yet to accommodate Phase II E911 location capabilities for wireless calls.[19] Even if the Commission were to consider NG911 requirements for wireless providers, there must be a recognition that PSAPs must have funding and technical support before they can receive and utilize the data provided by wireless carriers.

In some cases, the slow adoption rate of Phase II by PSAPs can be attributed to raiding of E911 funds by cash-strapped state legislatures.[20] Some state legislatures and city government have sought to increase E911 fees as a means of raising revenue for purposes unrelated to E911 deployment. In addition to slowing current E911 deployment, these activities endanger future funding for technical support and deployment of both E911 and NG911 systems. Under federal law, states are ineligible for federal 911 grant money if the state has misallocated 911 fees for unintended purposes.[21] Furthermore, the New and Emerging Technologies 911 Improvement

---

[18] *See, e.g.*, DOT NG9-1-1 Proof of Concept Report at 1-7, 4-12 (estimating the necessary investment and upgrade costs for IP-enabled infrastructure to be $11-13 billion over a 10 year period).

[19] *See, e.g.*, Public Safety Communications Division, State Chief Information Officer of California, "Wireless E9-1-1 Implementation Status: Statewide Totals", http://www.cio.ca.gov/PSCD/911/pdf/StatewideTotals.pdf (indicating that as of July 4, 2009 only about 87% of California had full wireless E911 capabilities) (last visited Nov. 9, 2009).

[20] *See, e.g.*, Linda Moore, Congressional Research Service, *An Emergency Communications Safety Net: Integrating 9-1-1 and Other Services*, at CRS-12 (Updated September 2005) (*available at* http://www.fas.org/sgp/crs/homesec/RL32939.pdf).

[21] ENHANCE 911 Act of 2004, Public Law 108-494 (2004).

Act of 2008 ("NET 911 Act"),[22] enacted in July 2008, limits state and local governments' authority to impose 911 fees only to where the fees will be used for their intended purpose. In the Commission's July 2009 report on the collection and distribution of 911 and E911 fees and charges by the states, the FCC noted that twelve states in 2008 reported using 911 funds to support programs other than 911 and E911.[23] In some cases, the slow adoption rate of Phase II by PSAPs can be attributed to raiding of E911 funds by cash-strapped state legislatures.[24] Unfortunately, 2009 is showing a similar trend with a significant amount of funds, collected under the auspices of 911, diverted to other non-related programs.

- In Wisconsin, the Governor supported and signed legislation diverting $20 million dollars in E911 funds to general revenue. Of note, four counties in Wisconsin haven't completed implementation of Wireless Phase I. [25]

- For the past several years, the Hawaii legislature has introduced legislation to reduce the 911 fee because the E911 Fund was becoming too large, however, a bill was never sent to the Governor's desk. Conversely, a bill introduced during the 2009 session to raid the Wireless Enhanced 911 Fund of $9 million, which was amended before passage to *increase* the diversion to $16 million, was signed by the Governor in May.[26]

- In Delaware, SB 69, signed into law on April 10, 2009 authorized the transfer of $4 million from the E911 Fund into the General Fund. The diversion of $4 million from the E911 Fund to the General Fund has placed in jeopardy plans for much needed improvements to Delaware's E911 system.[27]

---

[22] Public Law 110-283.

[23] Chairman Julius Genachowski, Federal Communications Commission *Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges* (Submitted Pursuant to Public Law No. 110-283) Page 9

[24] *See e.g.*, Linda Moore, Congressional Research Service, *An Emergency Communications Safety Net: Integrating 9-1-1 and Other Services*, at CRS-12 (Updated September 2005) (available at http://www.fas.org/sgp/crs/homesec/RL32939.pdf).

[25] Disbursement of Wireless 911 Fund Balance, Joint Committee on Finance, *available at* http://www.legis.state.wi.us/lfb/2009-11Budget/Budget%20Papers/666.pdf (last accessed June 30, 2009).

[26] *See* http://www.capitol.hawaii.gov/session2009/bills/SB884_CD1_.pdf (last accessed November 12, 2009)

[27] An Act Reverting Certain Funds of the State and Depositing Certain Funds of the State to the General Fund, SB No. 69, *available at* http://legis.delaware.gov/LIS/lis145.nsf/vwLegislation/SB+69/$file/legis.html?open (last accessed Nov. 12, 2009).

- In March of 2009, the Oregon legislature approved a $3.1 million transfer of E911 fees. The budget "rebalance" plan removed $3.1 million from an account aimed at improving 911 services, and $500,000 from an account to replace outdated 911 equipment.[28]

- In 2009, the Georgia legislature redirected $7 million from the 911 fund to support general revenue.[29]

NG911 deployment is certain to be challenging, and public safety will surely suffer if misappropriation of 911 funding is not stopped.[30]

III. CYBER SECURITY IS A GROWING ISSUE THAT HIGHLIGHTS THE NEED FOR REASONABLE NETWORK MANAGEMENT OF WIRELESS SYSTEMS

The *Public Notice* seeks comment on cyber security and the efforts being taken by communications providers to prevent, detect, and respond to cyber attacks.[31] Estimates of the damage from today's cyber attacks in the United States range from the billions to the hundreds of billions of dollars per year.[32] Although estimates vary, it is clear that companies and governments spend huge amounts of money securing networks from attacks. Yet, computer-based attacks, from individual parties and botnets,[33] appear to have grown markedly in recent years. November 2008 saw the emergence of Conficker, which quickly became one of the most widespread computer viruses ever.[34] Conficker has spread rampantly and evaded attempts by industry, academia, and government to neutralize it. It is now estimated to have taken over more than five million PCs.[35] Although the Conficker worm has not engaged in any large-scale

---

[28] Oregon SB 581at 5, *available at* http://www.leg.state.or.us/09reg/measpdf/sb0500.dir/sb0581.a.pdf (last accessed Nov. 12, 2009).

[29] *See* Dialing for Dollars, *available at* http://www.governing.com/archive/eletters/technology/2009/0906techletb.htm (last accessed Nov. 12, 2009).

[30] *See* DOT NG 911 Proof of Concept Report, 1-4 and 5-3.

[31] *Public Notice* at 3.

[32] Martin C. Libicki, RAND Project Air Force, *Cyberdeterrence and Cyberwar* at xv (2009) *available at* http://www.rand.org/pubs/monographs/MG877/ (last visited Nov. 9, 2009).

[33] In the cyber security context, a "botnet" is a network of computers, referred to as "zombies," infected with a program that allows them to be controlled remotely by the program's originator.

[34] *See* John Markoff, "Defying Experts, Rogue Computer Code Still Lurks", NY Times (Aug. 26, 2009) *available at* http://www.nytimes.com/2009/08/27/technology/27compute.html (last visited Nov. 9, 2009);

[35] *Id.*

malicious behavior at this time, if it were to activate all of its controlled systems it would have more computing power than any single facility run by the government or Google.[36]

With the growth in popularity of mobile broadband services, cyber attacks are more likely to move from the wired to the wireless world. As wireless devices gain more robust access to the Internet, cyber threats increase. Although not yet reaching the levels of sophistication found in PC-based worms and viruses, security threats against mobile devices are beginning.[37] Recently, hackers have demonstrated potential vulnerabilities in various smartphones similar to those historically seen in PCs.[38] Fortunately, mobile broadband networks, which are closely monitored by network operators, and wireless devices, which run on many different operating system platforms, have a well-deserved reputation for being highly secure compared to other means of Internet access.[39]

Wireless service providers have extensive market incentives to invest in state of the art cyber security measures. In the highly competitive U.S. wireless industry, network operators are constantly competing on the basis of network coverage, reliability, and service quality. Spammers, cyber attackers, botnets, and other hackers have the potential to severely disrupt wireless networks through unwanted network traffic and malicious code that could harm consumers by damaging the network or endangering subscriber data. Wireless providers, to date, have been successful in combating many of these risks. Unless wireless service providers

---

[36] *Id.*

[37] *See* Warwick Ashford, "'Zombie' Cellphone Networks Coming Soon," New Scientist (March 9, 2009) *available at* http://www.newscientist.com/article/dn16724-zombie-cellphone-networks-coming-soon.html (last visited Nov. 9, 2009).

[38] *See id.*; *see also* Andy Greenberg, "How to Hijack 'Every iPhone In The World'", Forbes (July 28, 2009) *available at* http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html (last visited Nov. 9, 2009); Kim Zetter, "First Ever iPhone Worm Rick Rolls Australia", Wired (Nov. 9, 2009) *available at* http://www.wired.com/threatlevel/2009/11/iphone-worm/ (last visited Nov. 9, 2009).

[39] *See* Bob Tedeschi, "Cellphones Largely Immune to Viruses, for Now", NY Times (Aug. 12, 2009) *available at* http://www.nytimes.com/2009/08/13/technology/personaltech/13smart.html?_r=2&ref=technology (last visited Nov. 9, 2009).

actively respond to these constantly morphing and growing challenges with dynamic and secure infrastructure protections, customer confidence will suffer – leading to loss of subscribers and revenue.

To continue to protect users from malicious activity and provide subscribers with the mobile broadband experience they demand, wireless network operators require flexibility to manage their networks in a dynamic and adaptive way that is responsive to the constantly changing threats they face.[40] Wireless service providers, to defend against cyber security threats, utilize a number of industry best practices to reasonably manage their networks from cyber attacks. Additionally, network operators have the benefit of the extensive best practices promulgated by the Network Reliability and Interoperability Council ("NRIC"), which issued

---

[40] There are three principal laws that broadly permit service providers to protect their rights or property as well as customers from fraudulent or abusive practices. First, Section 2511(2)(a)(i) of Title 18 permits a service provider to intercept, use and disclose wire or electronic communication to protect its rights or property. It provides that it shall not be unlawful for: an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. 18 U.S.C. § 2511(2)(a)(i).

Second, Section 3121(b) of Title 18 permits a service provider to install and use a pen register or trap and trace device **(1)** relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or **(2)** to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service. 18 U.S.C. § 3121(b).

Third, under Section 2701(c) of Title 18, the Stored Communications Act, a service provider may access electronically stored communications for any reason and further, under Section 2702(b) and (c), disclose communications or customer records "as may be necessarily incident to the rendition of service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2701(c).

Taken together, these sections implement a framework designed by Congress to ensure service providers had the flexibility to protect their networks from misuse or violation of a user's subscription rights. These provisions have been preserved and expanded over the past 50 years despite numerous amendments in and changes to the law. And, these statutory protections for service providers reflect nearly another 50 years of prior court decisions, which found broad rights for service providers to protect their rights or property from subscriber misuse or trespass. *See United States v. Beckley*, 259 F. Supp 567 (N.D. Ga. 1965) and cases cited therein.

more than 200 recommendations pertaining to cyber security.[41] Wireless network operators also collaborate with various Federal and local agencies on cyber security and network reliability issues. For example, CTIA and carriers work closely with the National Communications System ("NCS") and the United States Computer Emergency Readiness Team ("US-CERT") to share information when unusual activities are detected and to make changes in their networks to minimize vulnerabilities.

As was discussed extensively at the Commission's September 30, 2009 broadband workshop on cyber security, cyber attacks are fluid and ever evolving, so methodologies and practices also must be dynamic to respond immediately to new threats.[42] Any static defense is likely to be defeated and exploited – meaning that wireless service providers must be constantly vigilant in defending networks from attacks. As further indicated at the cyber security workshop, the speed of threats has increased to such a point that malicious code is typically found on the network within hours of identifying a vulnerability in a piece of software.[43]

One form of network management that subscribers have come to expect and embrace is spam blocking, which wireless carriers provide to protect both email and text messaging. As described at the cyber security workshop, however, there are a variety of other protective activities being engaged in 24 hours a day by network operators. These techniques include monitoring of traffic patterns from known origins of malicious activity (*i.e.*, botnets, spam

---

[41] *See* "NRIC Best Practices", https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm (last visited Nov. 9, 2009). CTIA also applauds the Commission on rechartering the Communications Security, Reliability, and Interoperability Council ("CSRIC"), whose recommendations are certain to provide another equally useful set of tools for wireless providers to employ in securing their networks. *See* Public Notice, "FCC Announces Membership of the Communications Security, Reliability, and Interoperability Council (CSRIC)", DA 09-2297 (rel. Oct. 26, 2009).

[42] *See generally* Remarks at the Cyber Security Workshop (Sept. 30, 2009) *transcript available at* http://www.broadband.gov/docs/ws_26_cyber_security.pdf (last visited Nov. 9, 2009).

[43] *See* John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, Remarks at the Cyber Security Workshop at 17 (Sept. 30, 2009) *transcript available at* http://www.broadband.gov/docs/ws_26_cyber_security.pdf (last visited Nov. 9, 2009) ("Nagengast Comments").

generators, etc.), as well as the tracking of different trends on the ports of the networks themselves. Network management techniques must be flexible and keyed in to the realities of network activity. For example, while some surges in network activity are the result of legitimate activity – such as the spikes in SMS traffic associated with the airing of American Idol – other surges could be caused by an ongoing distributed denial of service attack.[44] Wireless providers and manufacturers are constantly responding to newly identified vulnerabilities as quickly and efficiently as possible, however, it is impossible to stop every attack. Ultimately, the best defense, in addition to reasonable network management to protect against such threats, is to educate wireless consumers as best as possible about new threats and safe network usage – something that CTIA and its members are actively pursuing.[45]

IV. THE COMMISSION AND OTHER FEDERAL AGENCIES SHOULD REMAIN FOCUSED ON THE COMPLETION OF SPECIFICATIONS FOR COMMERCIAL MOBILE ALERT SERVICES

The *Public Notice* seeks comment on the use of broadband technology as part of public emergency alert and warning systems.[46] CTIA and its members have been working diligently with the Department of Homeland Security and other agencies to develop and roll out CMAS functionality over the past two years. However, key CMAS specifications have yet to be finalized by the Federal government. For example, the specific technical interface between wireless providers and the Federal government – the "C Gateway interface" – has not been made available to the public, nor have the technical specifications for the "A" Interface. CTIA remains optimistic that this process is nearing completion, with such information possibly being provided within the coming days or weeks. We are concerned, however, that any efforts to modify CMAS

---

[44] *See* Nagengast Comments at 19-20.

[45] *See, e.g.*, http://newscenter.verizon.com/press-releases/verizon/2008/online-security-tools-from.html (last visited Nov. 10, 2009).

[46] *Public Notice* at 3.

requirements to encompass broadband capabilities, or to reinvestigate the insertion of FM chipsets into wireless devices as part of the solution, are likely to slow the process and cause harm to the deployment of an alerting system.

CTIA firmly believes that wireless broadband services hold potential for additional CMAS capabilities (*e.g.*, data/video functionality in addition to currently contemplated text warnings) that will greatly increase the effectiveness of the emergency warning system. The Commission's CMSAAC specifically contemplated the evolution of the CMAS system to embrace enhanced capabilities such as geo-targeting and multiple languages, as well as developments in network and device technology.[47] However, as CTIA has indicated elsewhere, it is imperative that the initial CMAS deployments occur before any significant evolution of CMAS begins in earnest, so that initial lessons can be learned.[48] The wireless industry is ready and prepared to work with the FCC and other interested federal agencies to discuss next generation CMAS capabilities and standards, following the successful completion of the existing CMAS efforts.

CTIA also notes that broadcasters have again begun efforts to have the FCC mandate FM receiver/chipset technology into mobile devices.[49] However, the CMSAAC already did consider any number of technologies for use in mobile devices for receiving emergency alerts, including FM chipsets, as well as video broadcasting, paging and satellite antennas and hardware. The CMSAAC looked into these various technologies and ultimately concluded that incorporating these additional technologies was not technically feasible or would not accomplish the goal of

---

[47] *See, e.g.*, CMSAAC Recommendations at 52 (§ 5.4), 57-58 (§ 5.7), 64 (§ 7.1).

[48] Comments of CTIA, *In the Matter of Commercial Mobile Alert Service Research, Development, Testing & Evaluation Request for Information*, Dept. of Homeland Security Solicitation No. HSHQDC-09-R-00105 at 5 (filed Aug. 14, 2009).

[49] *See* http://www.nab.org/xert/corpcomm/pressrel/releases/110609_FM_on_Cell_60.pdf (last visited Nov. 10, 2009).

reliable reception of alerts. Most tellingly, the Committee concluded that broadcast technologies like MediaFLO, Digital Video Broadcasting - Handheld (DVB-H), and FM/RBDS receivers are not considered part of the CMAS, but recognized that these technologies may provide supplemental alert information for the CMAS. It is important to note that this issue was discussed in detail at the Working Group level as well as the full Committee level, and there was significant broadcaster participation in both areas.[50]

More than two years after the completion of the CMSAAC efforts, broadcasters are raising an eleventh hour argument that FM chipsets should be placed into commercial wireless devices to receive emergency alerts. However, the technological issues surrounding such a suggestion are formidable and the broadcasters have not addressed how commercial wireless devices would be adversely affected by this proposal. Specifically, because FM radio frequencies are considerably lower in frequency than CMRS bands, FM chipsets present significant antenna/reception issues for the mobile devices.[51] Moreover, constant monitoring for an FM emergency alert signal would rapidly diminish the battery life of a mobile device. Finally, issues such as carrier election (how could a carrier elect to transmit alerts in whole or in part?), tuning or scanning the receiver to the appropriate FM radio station, geo-targeting (mobile alerts will offer greater precision not present in FM-based alerts), and costs associated with a mandate (costs are not solely limited to the cost associated with placing an FM chipset into mobile devices but also include integration costs, designing devices to notify users when an FM radio alert is received, testing, etc.) continue to be limiting factors when considering an FM-based emergency alert solution.

---

[50] Broadcaster members of the CMSAAC that participated in the process included National Association of Broadcasters, Texas Association of Broadcasters, Florida Association of Broadcasters, Michigan Association of Broadcasters, Association of Public Television Stations and The Weather Channel.

[51] While a number of wireless phones are available today with FM receivers, CTIA is aware of no wireless carriers delivering emergency alerts via radio to cellphones, which entails many more complex issues.

CTIA and the wireless industry have long supported the creation of a comprehensive alert service that ultimately can be transmitted on multiple retransmission media, including wireless. A complete public alert and warning system should explore the full range of communications media and devices, and in that way, radio and television, wireless, cable and satellite can all complement each other in a layered approach that can result in an effective alerting service. A technological mandate of a single, flawed solution for wireless emergency alerts is not consistent with Congressional intent nor is it in the public interest. CTIA strongly urges the Commission to not take any action to disrupt the carefully considered and adopted process in place for wireless emergency alerts.

V. CONCLUSION

CTIA and its member companies are proud of their history of cooperation with government and public safety entities and innovation in the areas of public safety, homeland security, and cyber security. The wireless industry looks forward to continuing its leadership in developing and applying new broadband technologies to each of these missions. In each case discussed above, the Commission and other regulators should refrain from prematurely confining future choices or prescribing a specific path of development based upon today's technology. Instead, regulators should work in coordination with industry and public safety and provide them with sufficient flexibility and resources to develop broadband systems that will serve the public

for years to come, while also enabling network operators to handle the dynamic daily challenges in these areas.

Respectfully submitted,

By: *\/s/ Brian M. Josef*

Brian M. Josef
Director, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Dated: November 12, 2009