

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

In the Matter of:)

Effects on Broadband Communications) PS Docket No. 10-92
Networks Of Damage to or Failure of)
Network Equipment Or Severe Overload)

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General
Counsel

Brian M. Josef
Director, Regulatory Affairs

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

Dated: June 25, 2010

TABLE OF CONTENTS

	Page
SUMMARY	ii
I. INTRODUCTION	2
II. SYSTEM CONTINUITY AND SURVIVABILITY ARE ESSENTIAL COMPONENTS OF WIRELESS NETWORK SERVICE OPERATIONS	4
A. Physical Damage.....	6
B. Redundancy.....	7
C. Severe Overloads	8
III. THE WIRELESS INDUSTRY HAS SUPPORTED EFFECTIVE PUBLIC SAFETY AND DISASTER PREPARATION INITIATIVES	9
IV. THE COMMISSION SHOULD RELY UPON THE COMPETITIVE MARKETPLACE TO ENSURE SYSTEM CONTINUITY	12
V. CONCLUSION.....	16
APPENDIX A: ELEMENTS OF THE CTIA BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM	

SUMMARY

The wireless industry takes very seriously its responsibility to provide reliable and effective communications during times of emergency and heightened demand. In these comments, CTIA seeks to inform the Commission of the steps the wireless industry has taken to ensure that survivability and service continuity are integrated as core design principles of wireless broadband infrastructure and business practices. CTIA respectfully submits that the Commission should support the efforts of the wireless industry to bolster network survivability by ensuring that wireless broadband service providers continue to have the flexibility needed to prepare for and respond to emergencies quickly, effectively and efficiently.

CTIA and its members have coordinated closely with Federal, State and local government officials to develop strategic plans for ensuring service continuity when it is needed most. For example, CTIA and other industry members actively participated in the Communications Sector Coordinating Council that assisted in the development of the U.S. Department of Homeland Security's National Infrastructure Protection Plan and Communications Sector Specific Plan. Through such activities, the wireless industry has demonstrated its commitment to fortifying and preserving the nation's critical communications infrastructure.

Disaster recovery planning occurs at all levels of the wireless industry and by all industry members. CTIA has led the industry in strategic planning for emergency situations through its Business Continuity and Disaster Recovery certification program. Through this program, wireless broadband providers have designed and implemented comprehensive strategies for how to address and quickly recover from catastrophic service disruptions. Wireless providers use a variety of techniques to manage these risks. To prevent service from being disrupted due to

physical damage, wireless network infrastructure is hardened according to specific local circumstances, and redundancy is installed throughout the network. When service disruptions do occur, wireless providers implement dynamic network management techniques to reroute traffic and redirect physical and network resources as needed to minimize interruptions.

The wireless industry also has been an active and responsible partner to the Commission and other governmental bodies in developing numerous special emergency communications services. Through its work on Enhanced 911, Wireless Priority Service, the Commercial Mobile Alerting Service, AMBER Alerts, and other initiatives, the industry has contributed key technological expertise and development resources to produce vital emergency services that will continue to be of invaluable support to the public safety and emergency response community.

As the Commission investigates the resiliency of broadband networks, it should keep in mind the wireless industry's demonstrated commitment to this goal and the progress that has already been achieved. To remain effective at responding to disasters and other instances of heightened demand, and to continue contributing to larger development efforts, the wireless industry requires sustained flexibility in its business practices and network management techniques. Emergency preparedness and disaster response are inherently localized efforts. The challenges of fortifying wireless networks and quickly responding to network outages depend substantially on the specific environmental, topographical, population and other characteristics of the network at issue. Any prescriptive regulations or industry-wide standards adopted by the Commission will be unlikely to sufficiently address the diverse situations encountered by wireless network operators, and may actually negatively impact carriers' efforts to maintain service throughout their network.

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

In the Matter of:)	
)	
Effects on Broadband Communications)	PS Docket No. 10-92
Networks Of Damage to or Failure of)	
Network Equipment Or Severe Overload)	

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® (“CTIA”)¹ hereby submits the following Comments in response to the Federal Communications Commission (“FCC” or “Commission”) Notice of Inquiry on the Effects of Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload.² The wireless industry shares the Commission’s belief that ensuring the survivability of broadband communications networks during times of emergency or severe overload is of paramount importance. In these comments, CTIA seeks to inform the Commission of the steps the wireless industry has taken to ensure that survivability and service continuity are integrated as core design principles of wireless broadband infrastructure and business practices. As the Commission continues to pursue its mission to “promot[e] safety of life and property through the use of wire and radio communication,”³ it

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, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

² See Effects of Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, *Notice of Inquiry*, 25 FCC Rcd 4333 (2010).

³ 47 U.S.C. § 151.

should support the efforts of the wireless industry to bolster network survivability by ensuring that broadband service providers continue to have the flexibility needed to prepare for and respond to emergencies quickly, effectively and efficiently.

I. INTRODUCTION

In the first two days of May 2010, over 13 inches of rain battered Middle Tennessee—more than double the amount ever previously experienced. The results of the rain were catastrophic, and the region will be recovering for years to come. The Cumberland River, which runs through the heart of Nashville, crested at nearly 12 feet above flood stage in that city, in addition to the hundreds of millions of dollars in property loss, hundreds of citizens were displaced and dozens lost their lives. During this tragedy, the wireless industry rallied to ensure that essential connectivity was maintained, demonstrating the effectiveness of the business continuity and disaster response plans that have been implemented throughout the industry. Indeed, although the flooding damaged infrastructure and caused power outages leading to disruption of many telecommunications services, wireless providers emerged with only relatively minor interruptions that were quickly resolved. Moreover, to assist in staying in touch with governmental officials, relief workers and family, wireless broadband service providers offered free cell phones and air time to affected citizens.⁴

That the wireless industry responded so quickly and effectively to the flooding in Middle Tennessee comes as no surprise. CTIA and its members have consistently recognized the key importance of network survivability both to their business models and to their larger role in American society. The wireless industry has made service continuity and disaster recovery a guiding principle that informs myriad decisions regarding network construction, staffing,

⁴ *Free Cell Phones Given to Flood Victims*, WSMV.com, <http://www.wsmv.com/news/23617708/detail.html> (May 20, 2010).

training, and technology development. Moreover, the industry has gone out of its way to participate broadly in numerous public-private partnerships and voluntary programs intended to strengthen the communications infrastructure of the nation and to develop innovative and life-saving emergency communications services.

As the Commission investigates the resiliency of broadband networks, it should be mindful that wireless broadband providers have repeatedly proven capable of responding to emergencies quickly and efficiently, and very often they are the key remaining tool for emergency communications or the first communications systems to be restored after a catastrophic event. Moreover, the industry has worked closely with the Commission and other governmental bodies to craft comprehensive response strategies and deploy innovative services to facilitate public safety communications when they are needed most. All of this has been made possible due to the operational flexibility that has allowed the industry to respond to emergencies dynamically and appropriately without any unnecessary governmental mandates. The Commission should avoid prescriptive regulations that may limit this flexibility and thus hinder the industry's ability to respond to the next major emergency. Instead, the Commission should build upon the excellent work it has done in coordinating service providers' responses and addressing equipment needs and other shortages in the wake of disasters such as the recent earthquake in Haiti. The Commission, and especially the Public Safety and Homeland Security Bureau, have been engaged with the industry in an effective way that has facilitated the provision of emergency communications when needed most. It should not abandon this progress now in favor of unnecessary and potentially counter-productive regulation of wireless network infrastructure.

II. SYSTEM CONTINUITY AND SURVIVABILITY ARE ESSENTIAL COMPONENTS OF WIRELESS NETWORK SERVICE OPERATIONS.

The wireless industry understands that continuity of service and survivability of broadband networks have societal importance that far exceeds the business model of any individual network operator. During the aftermath of major disasters, many individuals rely on wireless as their sole means of communication because of its mobile nature and the speed in which carriers are able to restore service to affected areas. The wireless industry not only accepts this responsibility, but has embraced it through multi-faceted efforts to create national strategies for survivability of its communications infrastructure and to develop and implement best practices for fortifying and restoring service to wireless broadband networks in times of emergency.

The wireless industry has been working for years with the Department of Homeland Security (“DHS”) on the National Infrastructure Protection Plan (“NIPP”). The NIPP is the product of the combined efforts of representatives from across the Federal, State and local governments and the private sector to “protect[] and ensur[e] the resiliency of the critical infrastructure and key resources (“CIKR”) of the United States.”⁵ In addition to contributing to the development of the overall NIPP, CTIA and other wireless industry members have taken active roles on the Communications Sector Coordinating Council (“CSCC”), collaborating with representatives of the government and other communications industry to develop the Communications Sector Specific Plan (“CSSP”).⁶

⁵ U.S. Dept. of Homeland Security, *National Infrastructure Protection Plan* at 1 (2009) available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

⁶ See U.S. Dept. of Homeland Security, *Communications Sector Specific Plan* (May 2007) available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf>.

The CSSP outlines a bold and innovative vision of public-private partnership “to establish a single strategic framework for protecting the Nation’s critical communications infrastructure” through the establishment of “a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry.”⁷ The CSSP outlined 7 main security goals for the communications sector:

- Goal 1: Protect the overall health of the national communications backbone.
- Goal 2: Rapidly reconstitute critical communications services after national and regional emergencies.
- Goal 3: Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans.
- Goal 4: Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event.
- Goal 5: Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector.
- Goal 6: Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decisionmakers in the sector.
- Goal 7: Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.⁸

In keeping with the CSSP’s emphasis on risk assessment and contingency planning, the wireless industry has spent considerable time and resources creating business continuity plans and developing and strengthening its ties with federal, state, and local disaster recovery officials. Indeed, planning for continuity of service in the event of a disaster has been an integral part of wireless carriers’ operations. As such, carriers have developed their own array of best practices to anticipate and resolve problems created by both natural and man-made disasters.

To encourage and facilitate careful planning through the industry, CTIA established a Business Continuity / Disaster Recovery Program (the key elements of which are attached hereto

⁷ *Id.* at 1.

⁸ *Id.* at 3.

as Appendix A) that provides a voluntary annual certification for wireless carriers who have met the planning standards and objectives necessary to ensure that they have prioritized service continuity and disaster recovery. The Program is based around ten key steps (with several requirements under each step) designed to take a company from consideration of a Business Continuity / Disaster Recovery program, through implementation and full-company adoption. CTIA's Program is comprehensive, providing guidance to companies through all stages of the process from project initiation to training and maintenance. One of the key strengths of CTIA's Business Continuity / Disaster Recovery Program is that it accommodates the individual risk assessment and decisionmaking that must be done by each network operator with respect to each network. Wireless broadband service providers are constantly assessing the strengths and vulnerabilities of their networks by examining the specific environmental, topographical, geographical, population and cultural circumstances that influence the network.

To better educate the Commission on past efforts by the wireless industry to ensure service continuity, CTIA discusses herein efforts to minimize physical damage to networks, redundancy efforts and methods used to handle system overloading.

A. Physical Damage

For wireless broadband, physical damage planning commonly includes wireless providers provisioning their cell sites and switches with back-up batteries and/or generators to power them when electrical grids fail. Beyond this, wireless providers typically fortify their facilities according to predictable local need. For example, wireless providers will harden cell sites to withstand hurricane force winds in "risk areas" such as hurricane zones and mobile switching centers will be built on pilings or located on upper floors of buildings to protect against flooding in flood-prone areas. This site-specific planning stems from the individual assessments

conducted by wireless providers and depends upon continued flexibility to implement the necessary protections for the particular locality.

To shorten recovery time in disaster situations, carriers regularly stockpile equipment and provisions, such as spare parts, heavy equipment, sandbags, and tarps. When there is advance notice to prepare for a specific event, carriers will stockpile additional supplies, re-check inventories, and ensure fuel tanks are at capacity. Carriers also pre-position crews and equipment nearby or at event sites. Carriers also will typically increase security measures and monitoring of network operations in executing their continuity plans. For example, carriers may post constant guards at key facilities, change access policies, and/or inspect cell sites and mobile switching centers more frequently. In addition, carriers may back-up switches and IT systems more regularly so they can be restored later if damaged. Finally, carriers will carry out regular disaster drills and/or training for personnel that will be deployed during a disaster.

B. Redundancy

Because of the careful strategic planning of wireless network operators, cell sites are not necessarily a “major single point of failure” in many areas, contrary to the suggestion of the NOI.⁹ Broadband wireless networks often have numerous cell sites in a market, many of which may overlap in order to provide maximum capacity. As such, failure at a cell site during an emergency may not lead to a loss of service if there is another cell nearby that can serve the area, although total capacity and data rates may be affected. Provided sufficient flexibility in network management techniques is maintained, network operators can take steps such as increasing power at nearby cells to boost coverage and make up for a single cell or group of cells that have been rendered temporarily inactive due to physical damage.

⁹ NOI at 4335.

Indeed, redundancy is a core design principle of mobile broadband networks and is provided through the ability of wireless switches to rapidly and dynamically reroute traffic based on needs and capacity constraints during times of potential overload. Redundancy also is accommodated during times of heightened demand or decreased network capacity through the provisioning of cellular base stations on wheels (“COWs”), cellular base stations on light trucks (“COLTs”) and other temporary base stations. As CTIA explained in its comments filed in response to National Broadband Plan Public Notice # 3, COWs are portable cellular base stations that are fully functional without the need for access to commercial power. Within these portable base stations is a full assortment of equipment to sustain base station operations: (1) a diesel generator to ensure that the system is capable of operating even without commercial power; (2) RF equipment such as antenna mounting equipment, antennas, base station controllers and switching gear; (3) air conditioning capabilities to ensure equipment does not overheat; (4) AC power connectivity, should there be the ability to connect to AC power; and (5) lighting and other needs to enable communications.¹⁰

C. Severe Overloads

As the above discussion makes clear, wireless network operators leverage a variety of tools and techniques in implementing their business continuity and disaster recovery plans. Severe network overloads are managed dynamically by wireless broadband networks, underscoring the critical need for carriers to retain this capability free of restrictions on network management practices. Wireless broadband network operators are able to track and manage network loads in real time, shifting network resources to needed areas as demanded by the

¹⁰ See Comments of CTIA, GN Docket Nos. 09-51, 09-47, 09-137 at 10-11 (filed Sept 22, 2009) (“CTIA NBP PN # 3 Comments”).

specific situation. In addition, as noted above, COWs, COLTs and other temporary transmitters can be rapidly deployed and utilized to increase capacity in times of network overloading.

Ultimately, the two keys to successful overload management are (1) sufficient access to spectrum and (2) operational flexibility. The Commission took an important step toward enhancing wireless network operators' ability to maintain service during times of heightened usage by setting a goal of making available 500 MHz of additional spectrum for mobile broadband within the next ten years.¹¹ In its future policy making, the Commission should keep in mind the wireless industry's need for significant operational flexibility with respect to its network management and other practices to properly ensure that wireless broadband services are available when they are needed most.

III. THE WIRELESS INDUSTRY HAS SUPPORTED EFFECTIVE PUBLIC SAFETY AND DISASTER PREPARATION INITIATIVES.

The wireless industry has been a highly effective partner to the Commission and other governmental bodies in developing innovative solutions for public safety and emergency communications. In addition to providing the essential functionality of sustained connectedness during times of disaster or communications infrastructure overload, the wireless industry has promoted the development of several specific communications services that will save lives and property during times of emergency. Among these are Enhanced 911, the Wireless Priority Service, Wireless AMBER Alerts, and the Commercial Mobile Alert Service.

Enhanced 911 ("E-911"). Since its inception, the wireless industry has been fully committed to ensuring wireless users' access to E-911 services. The industry has invested substantial personnel resources and billions of dollars upgrading E-911 services, enabling carriers to route emergency calls to the nearest Public Safety Answering Points ("PSAPs") and

¹¹ See FCC, *Connecting America: The National Broadband Plan* at 86 (2010).

identify the caller's location through either network or handset-based methods. Wireless carriers also 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 more than 6,000 PSAPs that exist across the country. This ongoing commitment allows wireless consumers to make over 291,000 calls daily to 911. In many cases, wireless networks offer the most reliable means of contacting emergency services, as due to the redundancy of the networks and the ability to dynamically reroute traffic, 911 calls can be connected to a PSAP even where there is substantial damage to some portions of the wireless network.¹²

Wireless Priority Service. All communications networks become congested during a disaster. During such emergencies, however, emergency personnel must be able to communicate with each other to coordinate relief efforts. To address this congestion and essential public safety communications needs, the wireless industry has successfully implemented Wireless Priority Service ("WPS"). WPS is designed to give priority to key personnel during times of emergency. Although WPS has proven extremely effective during times of crisis, it has not been utilized to its full potential. Broader knowledge and education concerning priority access and utilization of commercial wireless networks by key government officials during times of crisis and high call volume will undoubtedly speed disaster recovery efforts. Accordingly, the Commission and the National Communication Service ("NCS") should initiate additional

¹² Indeed, wireless providers take their responsibility to deliver every 911 call very seriously. For example, when a recent outage by the landline telephone provider disrupted service to 911 call centers across Southeast Nebraska, wireless companies dynamically rerouted calls to cell phones being used by 911 call center operators. See Matt Olberding and Cory Matteson, *Windstream Prepares For Hearing After Massive Outage*, Lincoln Journal Star (April 2, 2010) available at http://journalstar.com/news/local/article_12c758e6-3ea9-11df-866d-001cc4c002e0.html. Wireless providers even dynamically monitored network traffic to ensure that emergency calls were completed. In one case, a wireless provider noticed a series of dropped 911 calls coming from the same number. Using location information technologies, the provider identified the location of the caller and contacted the appropriate emergency responders, who were able to respond to the caller. *Id.*

outreach efforts so that the government community is fully aware of the benefits of the Wireless Priority Service.

Wireless AMBER Alert Service. In 2005, the wireless industry enhanced its array of socially responsible public safety initiatives by offering Wireless AMBER Alerts™ to wireless customers through a partnership with the National Center for Missing & Exploited Children and law enforcement agencies. The Wireless AMBER Alerts Initiative is available, through participating carriers, to wireless subscribers in all 50 states, the District of Columbia, and Puerto Rico. With over 280 million Americans owning wireless phones, the alerts significantly increase the potential reach of the notification program. As such, Wireless AMBER Alerts have proven to be an invaluable tool in assisting law enforcement in the search process for missing children. Like Wireless Priority Service, the Federal government can help to educate citizens as to the existence of the AMBER Alerts service.

Commercial Mobile Alert Service (“CMAS”). When fully deployed, CMAS will provide Federal, State and local governments the ability send geographically targeted messages to the public containing emergency alert information related to imminent danger or Presidential emergency messages. The wireless industry was integral in developing the standards and technologies that will make the CMAS system a reality. Following the recent announcement of the adoption of design specifications for the development of the Federal Alert Gateway interface, participating wireless carriers are expected to test, develop and deploy the system by April 7, 2012.¹³ The wireless industry is ready and prepared to work with the FCC and other interested

¹³ See FCC’S Public Safety and Homeland Security Bureau Sets Timetable In Motion For Commercial Mobile Service Providers to Develop a System That Will Deliver Alerts to Mobile Devices, PS Docket No. 07-287, *Public Notice*, 24 FCC 14388 (2009).

federal agencies to discuss next generation CMAS capabilities and standards, following the successful completion of the existing CMAS efforts.

These public safety services play a crucial role in disaster response and other emergency situations. In each case, the public-private partnership effort was successful largely because the Commission has consistently prioritized flexibility and declined to mandate particular outcomes or technology. The alternative would almost certainly stifle innovation and result in less effective emergency communications. For example, application of a strict nondiscrimination rule with respect to wireless broadband services, as has been recently considered by the Commission,¹⁴ would seem to be directly at odds with the prioritization of certain government traffic during times of emergency under the WPS program, as well as the need to prioritize that would exist during certain types of emergencies (*i.e.*, pandemics). CTIA urges the Commission to keep this dynamic in mind during its ongoing policy making and to preserve the flexibility that has benefited the public interest through the development and deployment of robust and innovative emergency communications.

IV. THE COMMISSION SHOULD RELY UPON THE COMPETITIVE MARKETPLACE TO ENSURE SYSTEM CONTINUITY.

There is no incentive that the Commission could give that would be greater than a wireless broadband service provider's existing incentive to protect its significant network investment and customer confidence. Carriers understand that network survivability and disaster recovery must be core principles of their network design and business practices. As discussed above, the wireless industry has demonstrated its commitment to ensuring that its services are well protected during crises through voluntary, industry-based best practices.

¹⁴ Preserving the Open Internet, *Notice of Proposed Rulemaking*, 24 FCC Rcd 13064 (2009).

In light of these existing plans and partnerships, any efforts taken by the Commission should not be prescriptive. Individual carriers require flexibility to tailor their continuity plans to their own spectrum, infrastructure, population, topographical, resource and other challenges. What is reasonable under one scenario may be wholly inadequate elsewhere or at a different time. The Commission should not attempt to mandate the specifics of an effective network survivability strategy because the end result is nearly certain to be either too specific to be relevant to many network operators or too vague to be useful for all.

The wireless industry has repeatedly demonstrated its ability to effectively plan for and respond to emergency situations and other instances of significantly increased demand. For example, as detailed in the Report and Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks,¹⁵ and CTIA's comments filed in response,¹⁶ following Hurricane Katrina, wireless networks were instrumental in delivering core communications capabilities to both citizens and first responders. Over 25,000 phones were delivered to the area to provide wireless service. Despite near-term difficulties involving loss of power and backhaul,¹⁷ within one week after Katrina, approximately 80 percent of wireless base station sites in the affected area were up and running at full capabilities.¹⁸ Moreover, the Katrina Panel noted that more than 100 COWs were used to successfully restore service throughout the affected region.¹⁹ Text messaging provided by wireless providers was highlighted as a service

¹⁵ See Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, *Report and Recommendations to the Federal Communications Commission*, rel. June 12, 2006 at 9 ("Katrina Report").

¹⁶ Comments of CTIA, EB Docket No. 06-119 at 2-6 (filed Aug. 7, 2006).

¹⁷ Katrina Report at 9.

¹⁸ *Id.*

¹⁹ *Id.*

that offered communications even when voice networks became overloaded with traffic.²⁰ The resiliency of the wireless infrastructure allowed public safety responders, as well as the public, to have access to communications during the aftermath of the storm.

More recently, wireless providers have again stepped up to provide increased capacity and disaster recovery support in light of other major events and natural disasters. COWs and other temporary base stations were used strategically by wireless providers in the Washington, DC area to accommodate the tremendous increase in demand for wireless services during the inauguration of President Obama in 2009. In January of this year, after the island nation of Haiti was shocked by a 7.0 magnitude earthquake, wireless service was partially reactivated within 24 hours of the quake. Despite suffering substantial losses in personnel and property themselves, local wireless carriers had the majority of their network capacity restored within days.²¹ Thanks in part to the loan of dozens of temporary base stations from outside providers, the donation of tens of thousands of handsets by major carriers, and the provision of free international calling to and from Haiti, wireless communications were crucial in keeping Haiti connected to the world after the quake.²² Moreover, as discussed above, in the wake of the historic rainfall and flooding that assaulted Middle Tennessee in early May 2010, wireless networks were among the first communications services to be restored, and in many cases were never even interrupted.

CTIA and its members have consistently recognized the key importance of network survivability both to their business models and to their larger role in American society. Through

²⁰ *Id.*

²¹ See Suzanne Choney, *Firms Scramble to Repair Haiti Wireless Service*, MSNBC.com, http://www.msnbc.msn.com/id/34977823/ns/world_news-haiti_earthquake/ (Jan. 22, 2010).

²² *Id.*; see also Joey Samaniego, *T-Mobile USA Waives Call Charges to and From Haiti*, PC World (Jan. 14, 2010) available at http://www.peworld.com/article/186972/tmobile_usa_waives_call_charges_to_and_from_haiti.html.

substantial efforts to harden network facilities and planning, training and preparation for emergencies and other demand surges, the wireless industry has had unparalleled success in providing essential communications services when they are needed most. To the extent the Commission believes additional requirements are necessary, CTIA urges the Commission to respect wireless broadband providers' need for flexibility in responding to network survivability issues, without any mandated outcomes.

V. CONCLUSION

As detailed above, the wireless industry has thoroughly internalized the values of network survivability, business continuity and disaster recovery. The industry shares the Commission's commitment to providing a reliable communications system at all times, especially in times of emergency, when it is needed most. In its future policy making related to broadband survivability, CTIA respectfully requests that the Commission avoid prescriptive regulation and instead focus on preserving and promoting the flexibility that allows wireless broadband providers to best serve their customers and collaborate, as an industry, across the government to ensure that the nation's critical infrastructure is protected.

Respectfully submitted,

By: /s/ Brian M. Josef

Brian M. Josef
Director, Regulatory Affairs

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General
Counsel

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

Dated: June 25, 2010

APPENDIX A

Elements of CTIA – The Wireless Association’s Voluntary Business Continuity / Disaster Recovery Program

ELEMENTS OF CTIA – THE WIRELESS ASSOCIATION’S VOLUNTARY BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM

Requirement 1: Project Initiation and Management

Companies must demonstrate that they have done the following:

Defined objectives

Developed project plan and budget

Defined and recommended process structure and management

Obtained senior management commitment

Requirement 2: Risk Evaluation and Control

Companies must demonstrate that they have done the following:

Identified risks, events, and external surroundings that can adversely affect the company

Evaluated the damage that such risks and events could cause and probability of occurrence

Identified controls and safeguards to prevent or mitigate losses to company

Requirement 3: Business Impact Analysis

Companies must demonstrate that they have done the following:

Identified the critical functions of the organization

Identified the impacts resulting from disruptions and disaster scenarios

Determined recovery priorities and timeline objectives

Requirement 4: Developing Business Continuity Strategies

Companies must demonstrate that they have done the following:

Selected business recovery operating strategies

Assessed risk associated with each optional continuity strategy

Requirement 5: Emergency Response and Operations

Companies must demonstrate that they have done the following:

Developed and implemented procedures for response to situations

Established a process for activation of an Emergency Operations Center

Integrated Disaster Recovery/Business Continuity procedures with Emergency Response procedures

Established Command and Control procedures

Requirement 6: Developing and Implementing Business Continuity Plans

Companies must demonstrate that they have done the following:

Established and implemented Business Continuity and Crisis Management plans

Established procedures to transition from emergency response to crisis management / business continuity

Established a procedure to maintain and update Business Continuity plans

Requirement 7: Awareness and Training Programs

Companies must demonstrate that they have done the following:

Established a process to educate the company regarding business continuity issues and programs

Developed and presented training programs

Requirement 8: Exercise Business Continuity Program

Companies must demonstrate that they have done the following:

Established a process to drill/exercise the Business Continuity / Disaster Recovery program

Organized and completed exercises/drills

Developed and monitored after-action reports and results of exercises

Requirement 9: Public Relations and Crisis Coordination

Companies must demonstrate that they have done the following:

Developed plans to communicate with employees and management

Developed process to communicate, if necessary, with other stakeholders

Requirement 10: Coordination With External Agencies

Companies must demonstrate that they have done the following:

Established applicable procedures and policies for coordinating response with government representatives

Source: Copyright 2004 DRI International – Reprinted with Permission