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

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

COMMENTS OF AT&T INC.

Robert Vitanza
Gary L. Phillips
Paul K. Mancini
AT&T Inc.
1120 20th Street, N.W.
Washington, DC 20036
(202) 457-3076
Counsel for AT&T Inc.

June 25, 2010

SUMMARY

AT&T welcomes this opportunity to comment on the resiliency of broadband communications networks and their ability to withstand physical damage and severe overloads. The redundancies inherent in these networks – and other design and operational measures taken by broadband providers – facilitate infrastructure survivability. Indeed, in the current competitive broadband marketplace, network providers have strong incentives to ensure the survivability of their infrastructure. This has resulted in the deployment of broadband networks that are generally highly resilient in the face of disasters or severe overload situations.

The engineering design of wireline and wireless broadband networks is such that there are few single points of failure in the "core" and the aggregation (or "backhaul") sections of the networks. For example, the core of wireline broadband networks are typically designed in a "web" architecture with multiple pathways and multiple redundancies between various destinations. Similarly, wireless networks are designed with redundancies between switching offices and the core of the network as well as coverage redundancies in certain critical or high traffic areas served by the radio access network. Industry standards and best practices for engineering, installation and maintenance contribute to build in substantial resiliency for broadband network elements against physical damage. AT&T and other broadband providers also regularly monitor their networks and employ procedures to promptly detect and mitigate the effects of physical damage and to rapidly restore disabled network elements. And, when disaster strikes, AT&T's industry-leading Network Disaster Recovery program facilitates rapid service restoration. For its part, AT&T has made considerable investments in network survivability.

Broadband networks are also generally well-equipped to address events that may cause severe or prolonged congestion. Most modern broadband networks are "shared" in that they

support multiple users and uses over some or all of their underlying facilities (*e.g.*, voice, video and data; residential, business and government customers). Since not all users will use the network at the same time, network operators can use techniques like statistical multiplexing to provision sufficient bandwidth to support the "peak" demand on the network at any given moment. By designing their networks to be able to support predictable peak demands, network operators can offer services far more affordably than if they had to provision dedicated capacity to every individual user (regardless of whether the user is actually using the network), while still maintaining a high-quality experience for their users.

In the event of extremely high network usage caused by an unforeseen event, however, temporary congestion may be unavoidable. To prevent such temporary congestion from becoming severe or prolonged, broadband network operators design their networks with redundant paths in the network core to route traffic around congested nodes, impose traffic control measures and/or activate auxiliary equipment. Some broadband providers, including AT&T, also provision quality of service ("QoS") capabilities in their networks to ensure that, in the event of congestion, performance-sensitive traffic receives priority access to network resources. In particular, as wireline and wireless priority communications services developed for public safety, law enforcement and national security communications – known as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) – migrate to broadband platforms, we expect these QoS capabilities to play a vital role in ensuring these services are able to support the government's critical communications needs.

To the extent there are potential vulnerabilities in broadband networks that can inhibit communications in the event of physical damage to broadband infrastructure or a surge in traffic, these vulnerabilities are typically found closer to the network edge. For example, the last mile of broadband networks is generally not characterized by the same level of redundancy as the network core. However, physical damage near the network edge will typically affect only a small number of customers and will not impact the functioning of the rest of the network. Moreover, to the extent that certain users have mission critical communications needs and cannot tolerate temporary service outages (*e.g.*, some government or business users), broadband network providers are typically able to provision redundant and/or physically hardened facilities to meet their needs – provided, of course, that those users request such capabilities from their providers. Thus, AT&T believes there is a useful role for the FCC to play in educating these users about the importance of assessing their critical communications needs and ordering the appropriate services from their providers.

Because broadband networks are generally well-protected against localized or distributed physical damage or severe overload, there is no need for regulatory intervention in network design or operation. Indeed, prescriptive government mandates could potentially preclude effective survivability measures arising from technological improvements, provider experience, or the unique needs of various areas, potential threats, or specific networks. Such mandates could also impose unnecessary costs that adversely affect the affordability of broadband for many Americans. Further, even if it was inclined to impose such mandates, the Commission has not identified any specific authority that would permit it to regulate broadband network design and operation. Thus, AT&T believes the Commission can most effectively advance its survivability goals by encouraging industry efforts to adopt best practices, making more

spectrum available for wireless broadband, and educating users to reduce potential vulnerabilities at the edge of the network.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BROADBAND NETWORKS IN GENERAL ARE WELL-PROTECTED AGAINST PHYSICAL DAMAGE 3

A. Broadband Networks Are Engineered to Be Redundant at the Core, Minimizing the Effects of Any Single Point of Failure 4

1. Wireline Broadband Networks Are Designed to Minimize the Impact of Any Single Point of Failure 4

2. Wireless Broadband Networks Are Designed and Operated to Maintain Continuity of Communications 6

B. AT&T Has Adopted Procedures to Protect Its Network Against Physical Damage and Minimize Any Adverse Effects 9

1. AT&T Installs and Maintains Its Network to Help Ensure Continued Operation in the Event of Physical Damage to Network Facilities 9

2. AT&T Has Developed Disaster Response Measures That Rapidly Restore Damaged Networks and Communications in Disaster-Stricken Areas 11

C. There Are Numerous Procedures in Place That Help Ensure Survivability for Use by First Responders and PSAPs 16

III. BROADBAND NETWORKS ARE GENERALLY WELL-EQUIPPED TO HANDLE CONGESTION 19

A. AT&T's Network Design Helps Ensure That a Surge in Traffic Will Not Overwhelm the Network 19

B. Capacity Vulnerabilities Are Found Primarily at the Network Edge 22

IV. NETWORK SURVIVABILITY IS MOST EFFECTIVELY ADDRESSED BY THE PRIVATE SECTOR, WITH COMMISSION ENCOURAGEMENT OF INDUSTRY STANDARDS-DEVELOPMENT EFFORTS, SPECTRUM AVAILABILITY AND CONSUMER EDUCATION 23

A. The Commission Has Not Identified Legal Authority to Impose Network Design and Operation Requirements on Broadband Providers 23

B. There Are Appropriate Steps the FCC Can Take to Promote Survivability of Broadband Networks 24

V. CONCLUSION 27

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

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

COMMENTS OF AT&T INC.

AT&T Inc., on behalf of itself and its affiliates ("AT&T"), respectfully responds to the Federal Communications Commission's ("FCC" or "Commission") Notice of Inquiry ("NOI") seeking comment on the ability of existing broadband communications networks to withstand localized or distributed physical damage or severe overloads.[1]

I. INTRODUCTION

In its NOI, the Commission seeks to "enhance its understanding of the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability to failures in network equipment or severe overload conditions."[2] AT&T,

---

[1] *Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, Notice of Inquiry, FCC 10-62 (Apr. 21, 2010) ("NOI").

[2] *Id*. at ¶ 3. As an initial matter, we note that the Commission has not defined, or even attempted to explain, the term "broadband communications networks," nor has it identified specific broadband services on which it intends to focus. Before advancing past the NOI stage of this proceeding, we strongly encourage the Commission to identify the specific networks and/or services at issue so that it can develop a more focused record and appropriately tailor any policies it adopts for those networks/services. For purposes of these comments, AT&T will presume that the Commission is seeking comment on wired and wireless broadband networks capable of supporting telecommunications services and/or information services at speeds of more than 200 Kbps in at least one direction.

like Commissioner Baker, "is pleased that [the Commission has not] prejudged any affirmative regulatory role for the Commission in addressing network survivability."[3] Indeed, experience shows that existing broadband networks generally function effectively and are well-protected against threats of physical damage and severe overload. The redundancies inherent in these networks – and other design and operational measures taken by providers – facilitate infrastructure survivability in disasters or severe overload situations by enabling traffic to be routed through alternative pathways. Although the capacity of wireless broadband networks is necessarily constrained by available spectrum, the design and operation of these networks nevertheless provides flexibility for operators to address most overload situations.

Today, network providers have the discretion to design and maintain their broadband networks in the manner that they determine best meets the needs of their customers. In the current competitive broadband marketplace, network providers have every incentive to ensure the survivability of their infrastructure. Especially for governmental and large business customers, reliability is a key criterion on which to base the selection of their broadband service provider. Intense competition for these and other customers ensures that broadband service providers continue to make reliability, survivability, and restoration a high priority.

Accordingly, there is no basis for the Commission to adopt regulations to facilitate broadband network survivability. Indeed, the imposition of specific requirements designed to enhance survivability is not only unnecessary but could thwart survivability goals. The variance in potential threats and geographic area requirements makes clear that a single or broad-based solution is no solution at all. Instead, broadband providers must retain flexibility to fashion

---

[3] *Id*. at Statement of Commissioner Meredith Attwell Baker.

solutions that effectively address potential threats to their particular networks. As the following sections illustrate, broadband providers are doing so very effectively.

II. BROADBAND NETWORKS IN GENERAL ARE WELL-PROTECTED AGAINST PHYSICAL DAMAGE.

The NOI seeks comment on a number of issues related to the survivability features and risks presented by the physical architecture of broadband communications networks, as well as the survivability of physical facilities in which network elements are located.[4] In general, the engineering design of wireline and wireless broadband networks is such that there are few single points of failure in the core and backhaul networks. Redundancies help ensure that, if one portion of the network is damaged, the network will usually continue to operate. Further, strong competitive incentives drive broadband providers to try to eliminate or minimize any vulnerabilities that remain. AT&T and other broadband providers regularly monitor their networks and employ procedures to promptly detect and mitigate the effects of physical damage and to rapidly restore communications to areas where network elements have been disabled. In fact, a number of AT&T's practices have influenced the development of industry-wide best practices adopted by the Network Reliability and Interoperability Council ("NRIC").[5] The result is that significant outages in broadband networks due to physical damage are rare.

---

[4] *Id*. at ¶¶ 10-11.

[5] The NOI correctly highlights the output of the NRIC in documenting the best practices associated with the survivability of physical facilities in which network elements are located. *Id*. at ¶ 10. AT&T has been a leader in NRIC and supports the role that NRIC (and now the Communications Security, Reliability and Interoperability Council or "CSRIC") plays in promoting a more secure national communications sector by consolidating proven vulnerability mitigation tools into the body of best practices. Over the years, NRIC has compiled an extensive list of suggested practices to assist the industry in sharing and learning from successful approaches. Retaining best practices as guidelines and not requirements will ensure that providers have the flexibility to fashion solutions that most effectively address potential threats to their particular networks.

A. <u>Broadband Networks Are Engineered to Be Redundant at the Core, Minimizing the Effects of Any Single Point of Failure.</u>

The NOI asks what the "major single points of failure" are in broadband architectures, what the impact of failure is on these points, and what measures are taken to minimize the presence of single points of failure in broadband architectures.[6] However, wireline and wireless broadband networks are typically designed in a manner that minimizes the likelihood that a single point of failure could impact the network overall.

1. Wireline Broadband Networks Are Designed to Minimize the Impact of Any Single Point of Failure.

Wireline broadband networks are designed with redundancies throughout the network core. AT&T's core wireline network, for example, is designed with a "web" architecture so that there are multiple pathways to and from individual routers in the core, which provide alternate routes through which traffic can travel. As these alternate paths do not occupy the same physical link, damage to one path should not impact any others. The effect of this web-like design is that, if there is physical damage to one portion of the core network, data packets can be rerouted around the failure through one or more alternate paths. As such, a properly designed network will be able to withstand multiple points of failure in the transmission pathways within the network core because of the alternative routes available. Even when the rare outage occurs that affects multiple pathways at the same time, broadband providers generally employ sophisticated recovery technologies to quickly isolate, identify, and correct the problem.

The multiple pathways throughout the core of AT&T's wireline broadband network remain active at all times. AT&T's redundant paths are not "dark" paths,[7] but rather live paths

---

[6] *Id*. at ¶ 10.

[7] *Id*. at ¶ 14.

that are used during normal operation. This approach enhances the efficacy of the network, as it ensures that the condition of the path is always monitored and known. If a network were to employ "dark" paths to be used only in emergencies, problems with such a path would not be discovered until it was activated during the emergency situation – obviously the wrong time to discover a critical path failure. It also would be an extremely inefficient and wasteful use of valuable network infrastructure, with little benefit for the public.

Because the core of wireline broadband networks is designed as a web with alternate paths occupying different physical links, only a massive catastrophe that causes extensive physical destruction over a very large geographic area is likely to have a significant, long-term effect on network operations. Even then, however, communications between and among points outside the affected area should continue to function. Although short-term outages may occur on occasion, in general, broadband networks will continue to operate in the event of significant physical damage as long as the source and destination remain live.

The same is also generally true of the aggregation portion of wireline networks. For example, SONET rings between routers in a metropolitan area are generally bi-directional rings with automatic "fail-over." Equipment in the aggregation network – as in many other parts of the network – is also alarmed and continuously monitored for component failures. Most plug-in components have hot standby replacements. As a result, single physical incidents generally present minimal risk to regional or national communications.

The last mile of a wireline network is generally not characterized by the same level of redundancy as the network core.[8] For example, dedicated circuits between a residential

---

[8] *See also* Transcript of FCC Workshop on Critical Infrastructure and Information Collection at 26 (April 13, 2010) ("Critical Infrastructure Workshop Transcript"), *available at* http://www.fcc.gov/pshs/docs/critial-infrastructure-transcript.pdf (stating that the network core

customer's premises and the local Digital Subscriber Line Access Multiplexer ("DSLAM") are not redundant, nor is the DSLAM itself. Thus, significant damage to a dedicated circuit or the DSLAM that causes total or partial failure of the facility will likely affect service to the downstream customers.[9] However, no other parts of the network should be impacted by such an event.[10] Further, the number of customers impacted by such a loss or degradation of service would be relatively small.[11]

2. Wireless Broadband Networks Are Designed and Operated to Maintain Continuity of Communications.

As with wireline networks, wireless broadband networks are designed and deployed with redundancies to facilitate continuity of communications in the event of physical damage to a single point of the network. AT&T's network contains redundancies to minimize disruption in the case of physical damage. Much like AT&T's wireline network, the connections between

---

has the most resiliency and that "[a]s we start to get out to the edge is where it gets a little more difficult to manage").

[9] Redundancies are likely also lacking in customer premises equipment, including customer-owned switching and routing equipment used by large business customers. Damage to or other failure of this equipment could result in loss of service for such customers. However, the selection, installation, and servicing of such equipment is generally wholly within the customer's control.

[10] Of course, customers attempting to send or receive data from someone in the damaged area would not be able to reach them, but otherwise would have full functionality.

[11] While it is theoretically possible to design a network that provides redundant facilities from the core network all the way to the network-interface device at each and every residential customer's premises, doing so would be cost-prohibitive. Given the relatively small number of customers impacted by network edge failures – and the relatively low risk of such failures to begin with – undertaking these costs is simply not reasonable. This is especially the case given that one of the Commission's primary objectives in the National Broadband Plan is to increase the affordability of broadband for those who cannot afford it today. Broadband would be priced out of the reach of many existing and potential residential users if providers were required to invest in full network edge redundancy. Of course, for some government or business users with mission critical communications needs, the benefits of acquiring redundancy on an individual basis may be well worth the cost.

wireless Mobile Telephone Switching Offices ("MTSOs"), and between MTSOs and wireline switching offices, contain redundancies that protect traffic in the event of physical damage. Generally, the failure mechanisms in place in AT&T's wireless network are designed to move traffic from primary to back-up paths or elements very quickly upon the detection of a failure.

AT&T's wireless data core is comprised of fully redundant nodes and links that promote continuity of communications in the event of physical damage. Data services provided from a given data center location are designed to "fail-over" to other data centers in the event of an outage. AT&T engineers its networks with this "fail-over" capability by ensuring that there is sufficient capacity at any data center to serve its pro-rata share of additional traffic in the event another data center is lost.

Cell site backhaul transport links are a critical element to proper operation of a wireless broadband network. If one of these links fails, then the cell site it serves will go down.[12] While it is not economically viable to build physically diverse redundant cell site backhaul facilities to every cell site, AT&T closely monitors the availability and performance of all of its cell site backhaul transport links and holds regular service improvement sessions with transport facility providers. Further, by using optical fiber rather than copper facilities, wireless providers can both expand the capacity of their networks and minimize weather-related impacts to backhaul

[12] *See also* Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, *Report and Recommendations to the Federal Communications Commission*, at 9 (June 12, 2006) ("Katrina Panel Report") ("In general, cellular/PCS base stations were not destroyed by Katrina, although some antennas required adjustment after the storm. Rather, the majority of the adverse effects and outages encountered by wireless providers were due to a lack of commercial power or a lack of transport connectivity to the wireless switch (wireline T1 line lost or fixed microwave backhaul offline).").

links.[13] As in its wireline network, AT&T does not use "dark" backup links in its wireless network. It is also AT&T's policy generally not to deploy service over "collapsed rings" where the primary and backup circuits traverse the same path, as using multiple physical paths ensures survivability.[14] There are, however, instances in which there is no economically feasible alternative to placing primary and backup circuits in the same path.

Even where transmitters or cell site backhaul links may fail, wireless networks often contain coverage redundancies for certain critical or high traffic areas. In such areas, overlapping cell sites are available to pick up the traffic from sites that are not functioning. In such cases, customers should not experience a complete outage. They may, however, experience a deterioration of service quality due to higher than normal congestion. Because of spectrum constraints, it is generally not possible or practical to provide reserve capacity in the radio access portion of the network. Accordingly, AT&T continues to support the Commission's efforts to make available additional spectrum for wireless broadband services and believes the Commission would best meet its objectives in this proceeding by continuing to promote innovation, investment, and the allocation of additional spectrum for wireless services.

---

[13] Because glass does not conduct electricity, fiber facilities are not as susceptible to lightning strikes and electrical interference – major problems in the south and southeast during the summer months. Nor are fiber facilities as susceptible to water damage.

[14] As network protocols evolve to IP-based networks, the problems with "collapsed rings" become less of an issue. Unlike in a SONET-based TDM architecture, IP networks are "connectionless" in that routing is based entirely on the destination address of the data packet. Routers will use any physical facility connected to it to send packets forward, decreasing the risk that the primary path and alternative path are disrupted at the same time. The Commission should therefore take measures to facilitate the transition to next-generation IP-based networks and encourage innovations in network technologies and protocols.

B. AT&T Has Adopted Procedures to Protect Its Network Against Physical Damage and Minimize Any Adverse Effects.

Although AT&T's wireline and wireless broadband networks are designed to contain redundancies and to reduce vulnerabilities to physical damage, the company takes a number of additional steps to further protect its networks and facilitate prompt restoration. AT&T's installation and maintenance procedures help the network be better able to withstand physical damage when it occurs. AT&T has also developed significant disaster response measures that enable it to restore damaged networks rapidly when disaster strikes.

1. AT&T Installs and Maintains Its Network to Help Ensure Continued Operation in the Event of Physical Damage to Network Facilities.

AT&T's network installation and maintenance practices are tailored toward protecting its network elements against physical damage. As an initial matter, AT&T's critical network elements meet or exceed industry standards for continued operation when exposed to predictable environmental stresses such as earthquakes, fires, heat and airborne contaminants. In addition, AT&T's network cabling and framework infrastructure is designed to withstand high seismic activity, such as earthquakes, in accordance with industry standards. And, in hurricane zones and other areas of the country prone to capacity overloads, AT&T takes additional steps to design its infrastructure to maximize the availability of capacity options in an emergency. Specifically, AT&T requires that, at a minimum, critical equipment comply with the Network Equipment-Building System, which specifies requirements for, among other things, hardening equipment in various environments, including hurricane-prone areas.

Besides installing network elements that withstand physical damage, AT&T engages in maintenance activities that help ensure continued operation. For example, AT&T's Broadband Tools program monitors the condition of all lines and enables automated responses when problems are identified. Specifically, Broadband Tools contains a Real Time Loop Performance

Analyzer that looks at DSL performance and capacity and identifies issues even before they are reported by customers. This allows AT&T to quickly identify changes in network performance caused by physical damage and deploy repair personnel accordingly. AT&T also routinely installs battery backup and generators at major points of the network.

Additionally, AT&T takes steps to anticipate and prepare for potential future events. For example, in 2009, the Army Corps of Engineers examined the Howard Hanson Dam in Washington and noted that "[w]hile the dam itself is not in immediate danger of failing, there is increased risk to downstream communities until seepage issues with the right abutment have been addressed."[15] In response to this report, AT&T identified locations that could be impacted by flooding, rerouted voice and data traffic around the identified areas, identified microwave restoration solutions and procured appropriate equipment, identified cell sites immediately outside of the floodplain for augmentation, identified areas for mobility restoration equipment, if needed, and evaluated the relocation of physical network nodes for longer term solutions. AT&T also is working with local utilities in the area to plan for a potential flood event.

The Commission has specifically asked about network facility co-location and the risks it poses to survivability of infrastructure.[16] AT&T's practices with regard to the physical facilities in which its network elements are located also protect the network against physical damage. AT&T maintains two cable and two power entrances into each of its central offices for diversity, increasing the likelihood that the central office will remain operational if part of it sustains damage. AT&T does not co-locate diverse links from such offices in the same cable, further

---

[15] U.S. Army Corps of Engineers, Howard Hanson Dam, *at* http://www.nws.usace.army.mil/PublicMenu/Menu.cfm?sitename=HHD&pagename=mainpage (last visited June 12, 2010).

[16] NOI at ¶ 12.

contributing to survivability. AT&T also generally will not co-locate its facilities in another provider's building unless it meets AT&T's redundancy standards and employs personnel access controls to prevent unauthorized access to AT&T's facilities. In AT&T's view, this type of facility co-location is not inherently more vulnerable to physical damage than using multiple facilities if appropriate security precautions and redundancy measures are employed. Indeed, a secure co-location facility employing proper redundancy may be substantially less vulnerable than multiple, single-provider facilities with less security and/or fewer redundancies.

2. AT&T Has Developed Disaster Response Measures That Rapidly Restore Damaged Networks and Communications in Disaster-Stricken Areas.

While AT&T takes measures on a day-to-day basis to help ensure the physical survivability of its broadband network infrastructure, it must – and does – prepare for natural and man-made disasters that could cause damage to the network. By investing extensively in its disaster recovery program, engaging in regular training, preparing for imminent threats, and moving quickly after a disaster, AT&T generally is able to rapidly restore communications capabilities in case of any incident causing physical damage to its network.

Over the past 20 years, AT&T has invested over $500 million in its Network Disaster Recovery ("NDR") program and continues to invest in this initiative, through which AT&T strives to deliver the highest levels of service, quality, and reliability under most circumstances. This program has three primary goals: (1) to route traffic around affected areas; (2) to give the affected area communications access to the rest of the world; and (3) to recover communications service to a normal condition as quickly as possible through restoration and repair.[17]

---

[17] AT&T Network Disaster Recovery, *at* http://www.corp.att.com/ndr/ (last visited June 12, 2010).

AT&T's NDR program maintains an inventory of more than 300 technology and support trailers that can be deployed quickly to respond to disaster situations such as hurricanes, wildfires, and floods.[18] Specially-designed tractor-trailers are strategically located around the U.S. for dispatch, as needed, to act as a virtual network office. Each trailer has self-contained or dedicated power and environmental capabilities, and each houses a component of the network technology that would normally be a part of a permanent office. Once these trailers are deployed to a site, the individual components are interconnected to recreate the configuration of the damaged or destroyed network office.[19] In addition, AT&T's mobile command centers provide disaster response teams with fully equipped and controlled work space in the event of a disaster.

AT&T also supplies self-contained mobile cell sites – such as cells on wheels ("COWs") and cells on light trucks ("COLTs"), which can replace a failed cell site – and emergency communications vehicles that use a satellite link to provide voice and data service within 30 minutes of arriving on site.[20] AT&T maintains additional emergency equipment at designated locations, including portable generators, chillers, pumps and fuel cells at at-risk network offices, and permanent generators and battery backup at all wireless switches and many cell sites.[21]

---

[18] AT&T Vital Connections, Emergency Communications, *at* http://www.att.com/gen/general?pid=1325 (last visited June 12, 2010).

[19] AT&T Network Disaster Recovery, Recovery Equipment, *at* http://www.corp.att.com/ndr/team_equipment.html (last visited June 12, 2010).

[20] *Id*.

[21] Comments of AT&T Inc. – NBP Public Notice #8, GN Docket Nos. 09-47, 09-51, and 09-137, at 14 (Nov. 12, 2009).

The NDR program includes a team of more than 50 managers, engineers, and technicians, which has held at least three full-scale disaster recovery exercises each year since 1993.[22] These exercises "test as many of the NDR processes as possible, from the initial call out, to equipment transportation and setup, to technology turn-up and testing" and "team members are given hands-on training on new technologies and the recovery equipment is operated in field conditions."[23] AT&T designs these programs such that employees encounter various environmental conditions and different network asset restoration scenarios. After each exercise, results are reviewed to determine lessons learned, and new practices are adapted as appropriate to resolve future recovery events.[24]

In addition to engaging in disaster recovery exercises, AT&T employs a host of standard operating procedures to address certain disasters that can generally be predicted in advance, such

---

[22] AT&T Network Disaster Recovery, Recovery Exercises, *at* http://www.corp.att.com/ndr/exercises.html (last visited June 12, 2010).

[23] *Id.*

[24] So far in 2010, AT&T has conducted a recovery exercise in New Orleans, LA, in which the team tested three new technology trailers, a new power distribution trailer, and a new team rehab trailer. Recovery Exercise, 2010 – New Orleans, LA, *at* http://www.corp.att.com/ndr/exercises_2010q1.html (last visited June 12, 2010). AT&T's Special Operations Team held classes and hands-on training, and Operations team members received technology training at the site and first aid training at the team hotel. *Id*. AT&T also held a recovery exercise in the Detroit metropolitan area, intended to test and refine the NDR team's speed and efficiency in restoring network operations in the event of a disaster, and which "feature[d] more than 25 disaster recovery trailers and vehicles, including emergency communications vehicles, and a variety of smaller utility and support trailers, as well as a search-and-rescue dog team demonstration." Press Release, AT&T, "AT&T Recovery Exercise To Simulate Metro Detroit Network Disaster" (May 11, 2010), *available at* http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=30798 (last visited June 12, 2010). Most recently, AT&T provided a COW in Langley, Arkansas in response to flash floods in the Little Missouri River Caddo Gap area. This COW enabled emergency crews that lacked communications to respond to the flood and assist with recovery.

as hurricanes.[25] AT&T's pre-storm network preparations include adding capacity to the wireless network in the affected region, testing backup batteries at cell sites, distributing extended battery life and portable generators and maintaining existing fixed generators, topping off generators with fuel, using natural gas in some permanent generators to eliminate the need to refuel, and staging generators in safe locations for immediate deployment once a storm has passed.[26] AT&T also relocates its critical equipment to less vulnerable areas, elevates critical switches above expected flood levels, and protects its physical facilities against flooding.[27]

AT&T believes that strategic investments in disaster-prone areas promote network survivability in the event of a disaster. In 2006, after a number of Gulf hurricanes including Hurricane Katrina, AT&T's Mobility division invested $1.8 billion in network infrastructure in the Southeast United States, including $60 million in emergency-specific equipment. AT&T also continually engages in efforts to improve redundancy and recoverability in hurricane-prone areas.[28] In September 2008, these efforts paid dividends in the form of AT&T's highly successful response to Hurricane Ike in Galveston, Texas. In the wake of the storm, AT&T "quickly mobilized significant resources to repair damage from the hurricane, deployed generators to maintain network services in areas without commercial power, and support[ed]

---

[25] AT&T notes that while hurricanes can be tracked and predicted, there are storms, such as Hurricane Katrina, that cause damage far greater than could have been anticipated.

[26] Press Release, AT&T, "AT&T Stands Ready for 2010 Hurricane Season in Southeast" (May 17, 2010) ("2010 Hurricane Readiness Release"), *available at* http://www.att.com/gen/press-room?pid=17945&cdvn=news&newsarticleid=30827&mapcode=community (last visited June 12, 2010).

[27] AT&T Vital Connections, Emergency Communications, *at* http://www.att.com/gen/general?pid=1325 (last visited June 12, 2010).

[28] 2010 Hurricane Readiness Release.

evacuees."[29] AT&T's restoration efforts included deployment of 3,000 technicians, 200 construction contractors, 2,800 generators, 62,000 gallons of gas, 75,000 gallons of diesel fuel, and 13,000 gallons of propane to fuel generators.[30] AT&T also supplemented community support with a $250,000 grant to fund mobile Internet access centers. One week after the storm made landfall, wireless service had been restored to all of Galveston Island, with all permanent AT&T cell sites with 3G service on the island restored to operation and an additional portable tower deployed to support emergency operations.[31] Drive tests conducted through the storm-impacted area showed "near-normal wireless call completion rates."[32] Meanwhile, AT&T's deployed generators enabled more than 1,000 neighborhood terminals for wired voice, data and entertainment services to operate on backup power.[33] AT&T's video hub office for U-verse services remained operational throughout the storm.

AT&T is committed to restoring communications functionality to communities where network facilities may experience physical damage in the event of a disaster. Through its considerable investment in and careful planning for disaster recovery efforts, AT&T has helped to promote the survivability of its broadband infrastructure, as well as recovery in the event of damage. While AT&T's disaster preparedness and recovery capabilities may be industry-leading, broadband providers as a whole are likewise committed to ensuring the survivability of their networks during times of crisis or disaster. After all, survival of a provider's broadband

---

[29] Press Release, AT&T, "AT&T Restoration and Support Efforts Continue Following Hurricane Ike" (Sept. 19, 2008).

[30] *Id*.

[31] *Id*.

[32] *Id*.

[33] *Id*.

networks translates into survival of the provider itself. The Commission can provide no greater incentive than self-preservation. Thus, the Commission's survivability objectives would best be met by continuing to allow providers the flexibility to develop the most effective and efficient strategies for preserving their network infrastructure.

C. **There Are Numerous Procedures in Place That Help Ensure Survivability for Use by First Responders and PSAPs.**

The Commission has inquired as to provisions taken to help ensure the survivability of network services and cell sites for first responders and critical response agencies, such as PSAPs.[34] As an initial matter, AT&T notes that first responders often use their own networks, rather than commercial networks, for emergency communications. However, to the extent that first responders utilize commercial broadband networks, AT&T takes several steps to help ensure that these resources continue to be available to such entities in the event of an incident causing physical damage.

First responders utilizing AT&T's wireline and wireless networks benefit generally from the company's efforts to harden central offices and certain critical coverage cell sites. In addition, AT&T has designed its wireless network such that connections to critical response agencies are routed over diverse SONET rings, and network elements that handle traffic to these agencies are designed with internal redundancy. If a cell site is functional but the cell site backhaul is out, temporary microwave links can be established in a short time frame. AT&T's rapid deployments of mobile command centers, COWs, COLTs, and satellite services in emergencies help address demand for emergency communications services, including use by first responders. Most recently, in the Gulf region, AT&T deployed an emergency communications

[34] NOI at ¶ 10.

microcell and COLT, which were installed within 10 hours. Additionally, cell sites in any key area can be quickly equipped with an auxiliary generator to ensure a continuous power supply.

AT&T notes that critical response agencies such as PSAPs are primarily responsible for ordering and provisioning their own networks, and thus the resiliency of their networks is largely within the agencies' own control. However, local 911 wireline networks are generally designed for survivability using the same basic design principles that are used for the core network today. AT&T is willing and able to provide additional connection redundancies or contingency re-routing should the PSAPs contract for such services. Indeed, AT&T's contracts with federal customers often require access redundancies to critical facilities and mandate Telecommunications Service Priority ("TSP") in case of critical outages or new service installations. AT&T encourages critical response agencies to pursue a similar approach to ensure the survivability of their networks. AT&T is ready, willing and able to assist PSAPs and first responders by providing network facilities and services that will help meet their goals.

Beyond AT&T's network hardening steps, the federal government, working with service providers like AT&T, offers three priority service programs that support first responders and critical support agencies during emergencies. First, eligible participants in the TSP program receive preferential treatment when they need to add new lines or have existing lines restored following a disruption of service.[35] Second, the National Communications System's ("NCS's") Government Emergency Telecommunications Service ("GETS") provides priority access to eligible users over wireline TDM networks and "can be extremely beneficial during a major disaster or attack in which the public telecommunications networks are congested by high call

[35] FCC Public Safety and Homeland Security Bureau, Telecommunications Service Priority (TSP), *at* http://www.fcc.gov/pshs/services/priority-services/tsp.html (last visited June 12, 2010).

volumes and/or damage to the telecommunications infrastructure."[36] Third, the Wireless Priority Service ("WPS") operates in the same manner as GETS, but over wireless networks.[37] The President's National Security Telecommunications Advisory Committee ("NSTAC") has found that "[w]ith these services, [national security and emergency preparedness] users have a high probability of completing calls even during times of network stress."[38] As such, the Commission has stated that "[the three priority services] should be an important aspect of any emergency communications strategy, especially for those who rely on communications to respond to events and incidents on a daily basis and want to minimize their connectivity downtime."[39]

AT&T agrees that participation in these programs greatly assists critical response agencies and first responders in maintaining connectivity despite physical damage to network infrastructure. AT&T supports and is a strong advocate for all three of these programs. AT&T has long offered TSP restoration. AT&T's network is configured to ensure that authorized emergency calls have prioritized routing through GETS and WPS.

AT&T notes, however, that these priority programs do not yet extend to broadband services. NSTAC has observed that as IP technology "becomes more widespread and plays an

---

[36] FCC Public Safety and Homeland Security Bureau, Government Emergency Telecommunications Service (GETS), *at* http://www.fcc.gov/pshs/services/priority-services/gets.html (last visited June 12, 2010).

[37] FCC Public Safety and Homeland Security Bureau, Wireless Priority Service (WPS), *at* http://www.fcc.gov/pshs/services/priority-services/wps.html (last visited June 12, 2010).

[38] National Security Telecommunications Advisory Committee (NSTAC), Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic at ES-1 (Nov. 6, 2008) ("NSTAC IP-Based Traffic Report"), *available at* http://www.ncs.gov/nstac/reports/2008/NSEP%20IP-Based%20Traffic%20Report.pdf (last visited June 12, 2010).

[39] FCC Public Safety and Homeland Security Bureau, Priority Services, *at* http://www.fcc.gov/pshs/services/priority-services/ (last visited June 12, 2010).

increasingly important role in supporting [national security and emergency preparedness] services, [priority communications services] – and the network management techniques that make them possible – must be permitted to evolve in an IP-based environment."[40] AT&T is a major proponent of NCS' development of standards for prioritizing IP-based traffic and it urges the Commission to support this effort.

III. BROADBAND NETWORKS ARE GENERALLY WELL-EQUIPPED TO HANDLE CONGESTION.

As noted above, modern broadband networks are typically shared among many users and uses. As a result, broadband networks are typically designed to anticipate and absorb varying levels of network congestion without substantially impacting service quality. For its part, AT&T engineers its wireline and wireless broadband networks to high standards that maximize available capacity and minimize congestion during periods of heavy network use. This enables AT&T to provide continuous service during periods of significant congestion caused by extraordinary events.[41]

A. AT&T's Network Design Helps Ensure That a Surge in Traffic Will Not Overwhelm the Network.

Like other providers, AT&T's broadband networks generally effectively handle traffic surges because they are comprised of advanced network architecture and packet switched technology that enhance transport efficiency and mitigate performance degradation caused by congestion.[42] As noted earlier in these comments, the web-like core architecture in AT&T's

---

[40] NSTAC IP-Based Traffic Report at 13.

[41] AT&T also uses various network management techniques, including the provision of QoS capabilities, to address congestion events that may otherwise temporarily degrade the quality of a user's service experience.

[42] *See* Statements of Jeffrey Goldthrop, FCC, and David Keech, Frontier Communications, Transcript of Critical Infrastructure and Information Collection Panel, at 49 (April 13, 2010)

networks helps to address congestion issues by providing multiple routes for traffic to get from one place to another.[43] In a similar vein, AT&T's DSL service runs a dedicated point-to-point connection from each customer premise to the DSLAM. This design protects neighboring subscribers from impinging on each others' ability to access AT&T's network. To support its U-verse voice, video and Internet services, AT&T provisions a substantial amount of capacity in the aggregation portion of the U-verse network and also employs sophisticated QoS mechanisms to ensure performance-sensitive traffic receives the network resources it needs to provide a high quality user experience. Although AT&T's wireless network is constrained (like other wireless networks) by spectrum inputs, it can take steps to maximize its available capacity to address congestion issues by updating its equipment and employing frequency reuse where possible (albeit at significant expense).

AT&T and other broadband providers also address potential congestion problems by designing their networks' capacity based on forecasts developed from current and prior traffic patterns. AT&T engineers its wireline network to handle peak loads while still providing a high quality service experience, but generally operates at only a fraction of that level most of the time. To accomplish this, AT&T conducts time studies to determine the probability of capacity

---

("Mr. Goldthorp: How is moving to broadband IP-based technologies change[d] this . . . ? Mr. Keech: [I]t seems to be much easier to identify much more quickly that a problem is occurring, and we have surveillance tools that tell us immediately what . . . capacity changes . . . have occurred on any given link in any given portion of the network. We have just begun to implement technology that allows us to see the type of traffic that may be flowing over those lines, which gives you a much greater amount of information to begin to assess the nature of the problem.").

[43] As discussed in Section II, if a route fails, alternative routes will be chosen for the traffic. This will also occur if the primary path reaches a certain critical level of congestion (up until that point there could be some packet drop). However, AT&T is in the process of implementing technology that will route traffic around congestion, which should provide even more effective congestion-control measures for its network.

problems. Based on these efforts, AT&T then engineers its network and lines between central offices to operate at only a percentage of capacity. As a result, significant or prolonged congestion is rare. And when AT&T predicts that congestion will occur in the near-term – which usually is the result of growth or increased data use – AT&T takes steps to upgrade its network, such as through installing new digital loop circuits and other upgrades to its facilities.[44]

Similarly, AT&T engineers its wireless broadband network to provide optimal service during normal operations[45] and to tolerate some overload without adverse effects. AT&T continually monitors traffic loads at the nodal level. Based on its observations, AT&T defines recurring busy periods and projects traffic loads into the future. AT&T then engineers the nodes to provide high quality service during the busy periods. Specifically, AT&T establishes an engineering limit (*i.e.*, maximum capacity) and a relief threshold for each traffic-sensitive network element. As the traffic load approaches the relief threshold (*i.e.*, the trigger date), AT&T implements a relief plan to deploy additional capacity four to six months before the trigger date. Putting aside these engineering practices, however, AT&T recognizes that the availability of spectrum dictates the options available for traffic management at the edge of the wireless broadband network. The specific level of overload that can be accommodated will vary by location and by network element. When faced with very high levels of overload, a wireless network's service may deteriorate.

---

[44] This process generally takes 3 to 6 months.

[45] Consumers have benefitted from the wireless industry's emphasis on designing networks for "normal" traffic loads and not for events that generate abnormally high volumes of traffic. For example, if AT&T engineered its wireless network to handle the abnormal volume of text messages that are generated shortly after midnight on New Years Eve, AT&T would need to increase network capacity by approximately 350 percent. Designing networks for these isolated events would force wireless providers to shift significant financial and personnel resources away from more important projects, including rural build-out and 3G and 4G broadband deployment.

B. Capacity Vulnerabilities Are Found Primarily at the Network Edge.

While providers can design their networks and adopt practices to ensure sufficient capacity in high traffic events, congestion still occurs, particularly at the network edge.[46] This phenomenon is most acute among large business customers that lack the capacity to handle sudden increases in traffic in their last mile connections.[47] For example, large business networks may suffer from congestion when a company's employees abruptly shift to telecommuting and need remote access to corporate systems, such as during the blizzards that struck Washington, DC in 2010. Generally speaking, these capacity problems can be avoided if these businesses plan for such events and work with broadband providers to acquire the facilities and services necessary to support their communications needs in these circumstances.

For these reasons, AT&T has been advocating that large business customers conduct assessments of their anticipated network or remote access capacity now before an emergency situation, such as a pandemic, occurs. Should a large business anticipate additional capacity needs, these needs should be addressed promptly to ensure availability during the next

---

[46] *See, e.g.*, Statements of Jorge Magnana, Director, Level III Communications, Transcript of Critical Infrastructure and Information Collection Panel, at 23 (April 13, 2010) ("The points of congestion seems to be getting on the network. The capacity to get on the – you know, you can use the surface street to highway analogy where, you know, you can have a 12-lane highway, you don't necessarily build a 12-lane surface street to get to the 12-lane highway. So once you get to the core network the capacity is there. It's at the end points, it's at the edge as we go to broadband which will create the congestion points.").

[47] *See, e.g.*, Statements of Mareck Master, Telecordia Technologies, Transcript of Critical Infrastructure and Information Collection Panel, at 43 (April 13, 2010) (explaining that "most companies" suffer from traffic congestion problems when "everybody is at home and trying to work remotely" and "it turns out that at the far end the company is unable to support all these multiple users working – trying to work remotely. It's not the network that typically has the problem."); Statements of Martin, Transcript of Critical Infrastructure and Information Collection Panel, at 47 (April 13, 2010) ("These . . . are purely economic decisions, and in this particular case it's . . . [t]he Enterprise [that] has made the decision that it doesn't want to order a large pipe that is waiting and sitting there for that use one day a year, and it isn't the network.").

emergency. AT&T advises that, at a minimum, such pre-planning should include adding additional capacity to remote access networks or providing critical employees with intermodal Internet access from their residence.

IV. NETWORK SURVIVABILITY IS MOST EFFECTIVELY ADDRESSED BY THE PRIVATE SECTOR, WITH COMMISSION ENCOURAGEMENT OF INDUSTRY STANDARDS-DEVELOPMENT EFFORTS, SPECTRUM AVAILABILITY AND CONSUMER EDUCATION.

As made clear in the prior sections, broadband networks are generally well-protected against localized or distributed physical damage or severe overload. AT&T and other broadband network providers engineer and manage their networks with the objective of ensuring survivability and redundancy, so there is no need for regulatory intervention in network design or operation. Indeed, government mandates for prescriptive responses to survivability issues could potentially preclude effective survivability measures arising from technological improvements, provider experience, or the unique needs of various areas, potential threats, or specific networks. Such mandates could also impose unnecessary costs that could adversely affect the affordability of broadband for many Americans. AT&T believes the Commission can best advance survivability goals by encouraging industry efforts to develop best practices, making more spectrum available for wireless broadband, and educating users to reduce vulnerabilities at the edge of the network.

A. The Commission Has Not Identified Legal Authority to Impose Network Design and Operation Requirements on Broadband Providers.

The Commission has not identified any specific statutory basis for authority under Titles I, II, III or any other provision of the Communications Act that would allow it to adopt regulations prescribing how broadband providers design and operate their networks, as it is

required to do to support any rulemaking action.[48] Where, as here, it is not clear that there is such an explicit statutory grant of authority, the Commission should proceed with caution before seeking to impose prescriptive regulations that dictate how broadband providers run their networks.

B. **There Are Appropriate Steps the FCC Can Take to Promote Survivability of Broadband Networks.**

While regulations would not be appropriate – and indeed could be counter-productive – to fostering the survivability of broadband networks, the Commission can take other actions to advance survivability goals that would be consistent with the agency's statutory authority and the public interest.

First, the Commission should support the efforts of standards-setting groups. Multiple standards-setting organizations, such as the Alliance for Telecommunications Industry Solutions ("ATIS"),[49] the Telecommunications Industry Association ("TIA"),[50] the American National Standards Institute ("ANSI"),[51] and the Administrative Council for Terminal Attachments ("ACTA"),[52] provide useful fora for developing effective, flexible standards and best practices, including for broadband network survivability. To date, the Commission has had an open

---

48 *See, e.g.*, *Am. Library Ass'n v. FCC*, 406 F.3d 689, 689 (D.C. Cir. 2005) ("It is axiomatic that administrative agencies may issue regulations only pursuant to authority delegated to them by Congress."); *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010) (explaining that the FCC may exercise its "ancillary authority" "only if it demonstrates that its action . . . is reasonably ancillary to the . . . effective performance of its statutorily mandated responsibilities") (internal citations omitted).

49 Alliance for Telecommunications Industry Solutions, http://www.atis.org/.

50 Telecommunications Industry Association, http://www.tiaonline.org/.

51 American National Standards Institute, http://www.ansi.org/.

52 Administrative Council for Terminal Attachments, http://www.part68.org/.

invitation to many of these standards-setting meetings, but AT&T is not aware of FCC participation. Given the Commission's renewed emphasis on network sustainability, AT&T strongly encourages the Commission to contribute its unique insights to these fora, especially in light of their current focus on the unique attributes and needs of broadband traffic. The Commission should also continue to support and foster CSRIC as a helpful forum for information sharing and development of best practices. By relying on best practices and industry standards, rather than regulation, the Commission will allow competition to drive innovation in network survivability.[53] Providers compete based on the quality and reliability of their networks. Consequently, competition directly fosters survivability by creating strong incentives for providers to upgrade to more robust and resilient technologies.[54]

Second, as noted above, the ability of wireless broadband networks to address capacity overloads in the radio access network is limited to the amount of spectrum available to the provider in a particular area. With wireless broadband use surging – data traffic on AT&T's mobile network is up 5,000 percent over the past three years[55] – it is essential for the Commission to make more spectrum available for these services. The National Broadband Plan

---

[53] Further, regulatory intervention could create disincentives for voluntary and continual enhancement to standards, encouraging providers instead to wait and see what the Commission will do.

[54] Notably, the Commission's recently adopted "home roaming" rules are counterproductive to these efforts because the roaming rules discourage build-out and redundant networks. *See Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services*, Order on Reconsideration and Second Further Notice of Proposed Rulemaking, FCC 10-59, WT Docket No. 05-265 (April 21, 2010).

[55] Kris Rinne, Sr. Vice Pres. Of Architecture & Planning, AT&T, Remarks at the FCC Spectrum Workshop, at 11-12 (Sept. 17, 2009), *available at* http://www.broadband.gov/docs/ws_25_spectrum.pdf.

proposes to make 500 MHz newly available for broadband services within the next 10 years.[56] AT&T strongly urges the Commission to move forward promptly with these efforts as more spectrum will enable wireless broadband providers to be better able to address surging capacity demands and potential overload scenarios. AT&T also urges the Commission to develop technical and operational rules for all spectrum bands to be used for broadband service that maximize the spectrum's use for such service, such as by ensuring that the spectrum is paired, where appropriate, and avoiding rules that increase the risk of interference or the need to create an internal guard band within the service band.

Third, the Commission should encourage broadband users with mission critical communications needs to take preemptive steps to minimize vulnerabilities at the edge of the network. As noted above, the majority of communications failures during emergency situations or traffic surges result from vulnerabilities at the network edge – often due to the failure of large business users to have sufficient equipment or connections to address the needs of their employees. Accordingly, outreach efforts – conducted by the Commission as well as communications providers – are critical to educating such users on measures they can take to minimize these vulnerabilities and ensure their access to communications during emergencies. The Commission should also vigorously promote TSP, GETS and WPS and encourage the development of IP-based implementation of these services as they can be invaluable to maintaining and restoring communications for first responders and other critical public safety, law enforcement, and national security entities.

---

[56] Federal Communications Commission, *FCC Sends National Broadband Plan to Congress*, at 84 (March 16, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296880A1.pdf.

Finally, the Commission should refrain from adopting burdensome new reporting requirements. The Commission's existing Disaster Information Reporting System ("DIRS") provides an effective, voluntary mechanism for reporting communications infrastructure status and situational awareness information during times of crisis. DIRS streamlines the reporting process and enables communications providers to share network status information with the Commission quickly and efficiently.[57] No further data collection is required, particularly data about network problems that do not impact end users. Because a network can continue to function properly even with multiple points of failure, forcing communications providers to report network failures that do not impact consumers would be unnecessarily burdensome.

V. CONCLUSION

Broadband networks today generally function effectively and are well-protected against threats of physical damage or severe overload. Further, the highly competitive marketplace for broadband services will ensure that broadband providers remain committed to designing and managing their networks in a manner that promotes survivability in order to win and retain customers. While AT&T applauds the Commission's commitment to ensuring the continued survivability of broadband networks, it believes that the Commission would best fulfill its policy objectives by continuing to allow providers to design and deploy their networks without onerous regulation. Instead, the Commission should encourage industry standards-development efforts,

[57] Public Notice, "The FCC's Public Safety & Homeland Security Bureau Launches the Disaster Information Reporting System" (Sept. 11, 2007).

make more spectrum available for wireless broadband, and educate users to reduce vulnerabilities at the edge of the network.

Respectfully submitted,

AT&T INC.

By: *_/s/ Robert Vitanza_____*

Robert Vitanza
Gary L. Phillips
Paul K. Mancini
AT&T Inc.
1120 20th Street, N.W.
Washington, DC 20036
(202) 457-3076
Counsel for AT&T Inc.

June 25, 2010