



Mark J. Montano
Assistant General Counsel

1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3058 (telephone)
(703) 351-3158 (facsimile)
E-mail: mark.j.montano@verizon.com

July 7, 2011

FILED/ACCEPTED

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

.1111 - 7 2011

Federal Communications Commission
Office of the Secretary

RE: *Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket No. 11-60; Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92; Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, EB Docket No. 06-119*

Dear Ms. Dortch:

In response to the Commission's April 7 *Notice of Inquiry*,¹ Verizon and Verizon Wireless ("Verizon") are filing the attached comments in the dockets listed above. In our comments, Verizon discusses information considered confidential and proprietary. As such, Verizon is submitting the appropriate number of copies for public and non-public versions of the filing, along with the attached Request for Confidential Treatment. The non-public version of the filing is marked "Confidential – Not for Public Disclosure." Verizon will also electronically file the public version of these comments with the Commission via ECFS.

All inquiries relating to access to any confidential information submitted in this filing should be addressed to the undersigned.

Thank you for your assistance in this matter.

Sincerely,

/s/ Mark J. Montano

Encl.

¹ See 26 FCC Rcd 5614 (2011).

REDACTED FOR PUBLIC INSPECTION

No. of Copies rec'd 0+3
List A B C D E

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

FILED/ACCEPTED

JUL 7 2011

Federal Communications Commission
Office of the Secretary

In the Matter of)
)
Reliability and Continuity of) PS Docket No. 11-60
Communications Networks, Including)
Broadband Technologies)
)
Effects on Broadband Communications) PS Docket No. 10-92
Networks of Damage to or Failure of)
Network Equipment or Severe Overload)
)
Independent Panel Reviewing the Impact of) EB Docket No. 06-119
Hurricane Katrina on Communications)
Networks)
)

COMMENTS OF VERIZON AND VERIZON WIRELESS

Michael E. Glover
Of Counsel

Edward Shakin
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201

John T. Scott, III
Andre J. Lachance
VERIZON WIRELESS
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005

*Attorneys for Verizon
and Verizon Wireless*

July 7, 2011

REDACTED FOR PUBLIC INSPECTION

TABLE OF CONTENTS

I.	Disaster Preparedness Is a Priority for Verizon.	3
II.	Verizon’s Legacy Voice, Wireless, and Broadband Networks Have Features That Enhance Survivability.	4
	A. Legacy Voice and Wireless Networks	4
	B. Broadband	7
III.	Because Verizon Already Works Closely With the Federal Government During Disasters, the Commission Should Encourage Best Practices.	11
IV.	The Commission Should Encourage Backup Power Best Practices, Rather Than Revisit its Prescriptive Rules from the <i>Katrina Order</i>.	13
V.	The Commission Should Focus on Educating Broadband Customers.	17

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

In the Matter of)	
)	
Reliability and Continuity of)	PS Docket No. 11-60
Communications Networks, Including)	
Broadband Technologies)	
)	
Effects on Broadband Communications)	PS Docket No. 10-92
Networks of Damage to or Failure of)	
Network Equipment or Severe Overload)	
)	
Independent Panel Reviewing the Impact of)	EB Docket No. 06-119
Hurricane Katrina on Communications)	
Networks)	
)	

COMMENTS OF VERIZON AND VERIZON WIRELESS

Verizon and Verizon Wireless (“Verizon”) have long taken steps to ensure the availability and reliability of their services. To survive in the highly competitive marketplace, Verizon and other communications providers must be able to offer services that are available when customers wish to access them – even in the event of disasters or severe overloads. Verizon spends billions of dollars each year – estimated around \$17 billion – to build, maintain, and protect the health of its networks.¹ As Verizon’s CEO Ivan Seidenberg explained, “Our job is to make certain those networks are safe and reliable enough for the security of our nation – and our world – to depend on.”²

¹ See Ivan Seidenberg, Defense Information Systems Agency (DISA) Customer Partnership Conference, <http://www22.verizon.com/onecms/LeadershipTeam/Speeches/Speeches.htm> (Apr. 21, 2009).

² *Id.*

REDACTED FOR PUBLIC INSPECTION

As described in these comments, Verizon prioritizes disaster planning. Verizon's legacy voice, wireless, and broadband networks have significant redundancy and other protective measures in place to keep the networks up or to quickly restore them during disasters and severe overloads. Additionally, the government has entities already in place to work with communications providers to ensure that the government understands the impact of network-affecting events and is able to assist in a response, if necessary. Accordingly, the Commission should focus on continuing to foster public-private collaboration, such as the recently chartered Communications Security, Reliability, and Interoperability Council (CSRIC), to develop best practices that can adapt to evolving threats to help ensure that *all* providers have the most effective tools for network resiliency and survivability.

In particular, the CSRIC should examine the backup power best practice adopted in 2005 and consider whether it should be updated and extended to broadband networks. This best-practice approach would allow providers the flexibility to focus their resources on preparedness and recovery, rather than complying with prescriptive rules, such as those adopted in the *Katrina Order*, but that never went into effect.³

Finally, the Commission should help ensure that end users plan for disasters and overloads by taking steps where possible to address their specific communications needs.

³ See *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Order, 22 FCC Rcd 10541 (2007) ("*Katrina Order*").

DISCUSSION

I. Disaster Preparedness Is a Priority for Verizon.

Verizon has substantial experience in disaster preparedness and developing response procedures. Verizon has emergency response and recovery plans in place to address business continuity. Indeed, it is Verizon's written corporate policy to establish and maintain plans regarding continuity of operations and continuity of management, together with emergency operations centers, alerting lists, and alternative temporary locations deemed necessary to facilitate the installation, maintenance, and restoration of critical telecommunications or information services under conditions ranging from local emergencies to widespread disasters. Verizon's policy also provides that Verizon will participate in the National Coordinating Center for Telecommunications (NCC), which serves as the national point of contact for telecommunications emergency preparedness matters within the United States.

Verizon's overall emergency response and recovery efforts are managed at emergency operations "hubs" – the Verizon Emergency Operations Center (EOC), which can be activated at multiple locations, including Texas, New Jersey, or via a Mobile Command Center, and the Verizon Wireless EOCs located in New Jersey and Texas. When activated, the EOCs are staffed by members of Verizon's Business Continuity and Emergency Management teams, the Verizon Wireless Crisis Management Teams (CMTs), representatives from several Verizon departments, and Verizon's representatives to the NCC.

Verizon's business units have also divided the country into specific regions based on their respective business needs and established specific continuity programs and plans

that are appropriate for each of its regions. For example, one of Verizon's business units has a Regional Preparedness Plan for the Southeast Region that provides for appropriate equipment to be pre-positioned within a certain number of hours before estimated landfall of a hurricane. There is another Plan for the West Coast Region that includes procedures for, among other things, the aftermath of an earthquake. Similarly, there is a Plan for the New England Region that addresses contingencies for severe winter storms, including ice storms, which can lead to widespread power outages.

Verizon manages its response to disasters and emergencies through a Business Continuity Governance Structure comprised of four tiers of decision-making bodies – an Executive Policy Council, an Executive Steering Committee, three Executive Working Committees, and a Business Continuity Planning Committee. These Committees coordinate with Verizon's Cyber and Security team and the Verizon Wireless Business Continuity/Emergency Response team to establish appropriate business continuity policies, strategies, priorities, and guidelines. Verizon's Business Continuity Governance Structure also coordinates closely with other public and private organizations, including the NCC, the Commission, and other service providers.

II. Verizon's Legacy Voice, Wireless, and Broadband Networks Have Features That Enhance Survivability.

A. Legacy Voice and Wireless Networks

To best meet customer needs, Verizon sets an internal goal for the availability of its wireline and wireless voice networks. Verizon endeavors to maintain far greater than 99% availability and regularly achieves that goal.

To reach this ambitious goal, Verizon has long focused on service protection and restoration strategies for its networks.⁴ Verizon's legacy voice networks are comprised of numerous components that are connected using diverse (i.e., redundant) transmission systems, circuits, and network technologies. Verizon has the ability to re-route traffic dynamically over its networks to address outages at a specific location. This capability makes Verizon's networks more resistant to the impact of a local weather emergency or disaster.

Verizon typically employs fiber optic connections for backhaul transmission, using Synchronous Optical Networks (SONET) and Reconfigurable Optical Add Drop Multiplexor (ROADM) architectures. Both of these technologies have redundant paths. For instance, most of Verizon's SONET networks used for backhaul services are designed to have no commonality – i.e., the two paths are not located within 25 feet from each other – between the working and protect fiber paths beyond 500 feet from the central office. As a result, a diverse SONET ring should survive any single fiber cuts outside of the 500 foot radius from a central office. When protection is needed, the ROADM network implements a SONET architecture using one of the wavelengths so all the SONET benefits apply.

Verizon also maintains Network Operations Centers (NOCs) that monitor critical network facilities, including transmission facilities, switches, and cell sites across Verizon's networks. The NOCs are staffed 24 hours a day, seven days a week with experienced personnel who work closely with regional and local field operations teams

⁴ The descriptions in these comments are at a relatively high level to avoid providing wrongdoers with a roadmap that would allow them to circumvent Verizon's protective measures.

and with vendors to coordinate and expedite the restoration of service in the event of outages.

The NOC technicians work with the field operation managers, and personnel are dispatched to an affected site as needed. An inventory of standard spare parts and repair equipment is available to technicians in centralized network locations. Verizon also has standing agreements with critical vendors to get support 24 hours a day, seven days a week from their engineering personnel and to obtain replacement equipment if required.

As discussed in more detail below, Verizon typically employs automatic power backup systems for its key network equipment. These systems include large banks of batteries and diesel generators to charge those batteries. Verizon also has arrangements with fuel suppliers to refill fuel tanks as needed, thus allowing Verizon's critical network components to operate until commercial power is restored.

In addition, buildings housing Verizon's switches are designed to provide maximum protection for their systems and services. These buildings have automatic fire detection and suppression systems, as well as physical security systems and alarms to prevent entry by unauthorized personnel.

For its wireless networks, Verizon protects its cell site operations in many of the same ways, including redundancy in the equipment and backhaul connections, automatic power backup systems, automatic fire detection systems, and physical security systems and alarms. Through arrangements with vendors, the major components of the wireless networks – up to and including buildings and towers – become an immediate priority restoration effort on the part of both Verizon and its vendors.

In addition, Verizon designed its wireless network so that its cell sites in urban areas are overlapping. That is, if one site goes down, neighboring sites have capacity in place to handle the downed site's traffic. When necessary, Verizon can augment that capacity with portable cell sites referred to as cells-on-wheels (COWs) and cells-on-light-trucks (COLTs), which are fully functional generator-powered cell sites that can replace or enhance network coverage and capacity in a given area. Verizon's fleet of these portable cell sites, as well as portable towers, repeaters, microwave links, generators, and HVAC units, are strategically located all around the country and may be quickly deployed to an area that is affected by a weather-related or other disaster. In addition, all of Verizon's mobile switching centers and the vast majority of its over **BEGIN** **CONFIDENTIAL** **END CONFIDENTIAL** cell sites have alternative power supplies via battery backup and generators.

B. Broadband

Drawing from this experience as a provider of reliable voice services, Verizon deployed its broadband networks to minimize the risks that the networks would not be available. In many cases, particularly when the voice and broadband network components are located in shared facilities, the protections are the same.

Like its goal for the availability of its voice networks, Verizon sets an internal goal for the availability of its wireline and wireless broadband networks. That is, Verizon endeavors to maintain well over 99% availability for its broadband network infrastructure, even for its low-priced, "best efforts" broadband services. Verizon tracks its performance against its internal goals and makes changes in the networks, including purchasing new equipment and augmenting network capacity, to handle increased

consumer demand for bandwidth where required. With respect to its wireless broadband networks, Verizon closely tracks metrics for failed connection attempts and lost connections.

Verizon's broadband networks are also designed with a degree of redundancy. Verizon's wireline network is designed to be redundant all the way until the "last mile" to the customer premises. Specifically, for its residential broadband networks, Verizon employs dual-path redundancy from the Internet backbone through the metro backbone to the access router serving the last mile. Verizon utilizes two circuits in diverse pathways and houses the routers in physically separate buildings. Each of the dual paths can carry 100% of anticipated network traffic and is designed to automatically switch over in the event that one of the paths fails.

Moreover, even when both paths are available, Verizon's NOCs closely monitor broadband traffic for indications of congestion. Should traffic reach the internal relief threshold, Verizon will augment the path with additional capacity. An added benefit of this 100% redundant architecture is that the network is able to absorb a large shift in demand for bandwidth due to unforecasted events. Verizon also has processes for customer grooming, which involves rearranging circuits to ensure that facilities are being optimally utilized, to relieve potential overloads in any one given path. Finally, with respect to enterprise and government broadband customers, Verizon supports a range of services, including backup circuits, diverse entrance facilities at the customer premise, priority services, and physically diverse routing options, to ensure that such customers can purchase diverse circuits to meet their needs for continuity of communication.

As a result, widespread outages on Verizon's wireline broadband network are relatively rare. While outages may occur when a problem exists in the last mile, such outages would affect no more than 1,000 to 2,000 of the millions of customers served, with a majority of these events normally affecting even fewer customers. Because broadband networks are more distributed than traditional legacy networks, the number of customers potentially affected by any given network outage is typically far smaller than the number of customers potentially affected by outages on the voice network. By comparison, on the voice network, a single switch outage could affect tens of thousands of customers.

Verizon's wireless broadband network also has redundant assets to help ensure its availability to customers. As with its wireline network, Verizon employs dual path redundancy from the Internet backbone to the mobile switching centers and redundant Ethernet backhaul circuits to the wireless broadband cells. And as described above, Verizon's cell sites in urban areas are overlapping, and Verizon can rapidly augment capacity and coverage with wireless broadband-equipped COWs and COLTs.

Recent weather-related events demonstrate the reliability and survivability of Verizon's networks. For instance, in the wake of widespread and unusually violent weather that pounded the South and South Central states this spring, wireless network teams and their mobile assets converged rapidly on the affected areas and immediately began to replace mangled towers and damaged equipment shelters, restore power and backhaul, and recover both voice and broadband services for emergency responders and Verizon's customers.

Similarly, wireless network teams responded to record flooding in the Mississippi, Missouri, and Ohio River watersheds: relocating cell sites at risk, sandbagging others, and deploying mobile assets to maintain coverage and capacity in the affected areas. Verizon field teams have worked, and continue to work, closely with emergency management agencies at the federal, state, local, and tribal levels to ensure that Verizon's voice and broadband services continue to be available to customers and to provide backup for threatened emergency services networks.

Likewise, President Obama's Inauguration did not adversely affect Verizon's wireless networks despite increases in traffic levels of 100-200%. Verizon moved assets into place ahead of time to handle the expected traffic load. And on that morning, Verizon carefully monitored voice and broadband traffic in real-time and fine-tuned the network by adjusting the footprint of neighboring cell sites to pick up traffic from sites with surges of use. As a result, despite huge crowds and volumes of traffic, Verizon experienced a normal day's performance metrics on Inauguration day.

Finally, Verizon employs the physical security practices discussed above – including fences, access control systems, alarms and video surveillance – to guard its

generator systems. In the wireless broadband network, all of Verizon's mobile switching centers and the vast majority of its over **BEGIN CONFIDENTIAL** **END** **CONFIDENTIAL** cell sites have alternative power supplies via battery backup and generators.

III. Because Verizon Already Works Closely With the Federal Government During Disasters, the Commission Should Encourage Best Practices.

Verizon, like many other communications companies, has a close working relationship with the federal agencies and governmental bodies that monitor broadband networks. For example, the NCC, part of the National Communications System (NCS), facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications structure, including broadband networks. Verizon has three employees on-site with NCC to enhance Verizon's ability to share relevant status information about its networks should a catastrophic event occur.

In addition, Verizon is engaged with the Communications Sector Coordinating Council (CSCC), which works to protect the United States' communications critical infrastructure and key resources from harm and to ensure that the communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. The CSCC coordinates with the other 17 critical infrastructure sectors through the Partnership for Critical Infrastructure Security (PCIS) to address cross-sector issues and interdependencies. The PCIS provides senior-level cross-sector strategy coordination through a partnership with the Department of Homeland Security (DHS) and the sector-specific federal agencies or SSAs. Verizon is also involved with the

DHS-led coordinated watch and warning center aimed at improving national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure.

In light of the already-established government resources devoted to understanding the availability of networks during disasters, the Commission should continue to promote the establishment and updating of best practices that providers can adopt to better protect their networks. In 2010, the Commission took an important step towards that end when it re-chartered the CSRIC, an advisory committee consisting of public and private entities that provides guidance and expertise on the nation's communications infrastructure and public safety communications. The CSRIC should work expeditiously to recommend and publish best practices and actions that the communications sector can put into practice to ensure the survivability of broadband networks. There are various issues that the CSRIC should examine, including backup power, as explained below; access; backhaul redundancy; interconnected VoIP and broadband outage reporting; and 4G VoIP.

The Commission should not mandate best practices, however, for three reasons: (a) potential disasters evolve and prescriptive practices will be overcome by evolving threats; (b) mandates may discourage open participation and collaboration in future CSRICs; and (c) mandated implementation of best practices is not consistent with their intent. The technology Verizon deploys and the highly competitive marketplace in which Verizon competes is evolving so fast that regulatory requirements would be outdated shortly after they have been mandated, thus stranding capital in areas that do not achieve the Commission's survivability objectives.

Historical experience demonstrates the success of voluntary best practices relating to survivability. From 2004 through 2006, Verizon participated on the Network Reliability and Interoperability Council (“NRIC VII”) subcommittee on cybersecurity. The NRIC subcommittee created a report that documented over 200 best practices related to cybersecurity. The report analyzed existing cybersecurity best practices, such as identity management, messaging security, attacks, and wireless security. Along the same lines, NRIC has adopted best practices for a number of areas related to survivability, such as physical security, network reliability, and continuity. Although some of the best practices relate solely to legacy voice services, many of them are applicable to or can be easily translated to broadband. Verizon has implemented a number of these best practices on a broad scale for its wireline and wireless broadband networks and has found them to be effective in helping to better secure its networks from physical threats.

IV. The Commission Should Encourage Backup Power Best Practices, Rather Than Revisit its Prescriptive Rules from the *Katrina Order*.

In 2005, NRIC adopted a best practice relating to backup power with respect to voice service:

Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.⁵

As noted above, Verizon generally follows this best practice by ensuring availability of backup power for its key facilities through a mix of onsite batteries and generators,

⁵ See NRIC VII Focus Group 1C Final Report, *Analysis of the Effectiveness of Best Practices Aimed at E9-1-1 and Public Safety*, Best Practice 7-7-5204, <http://www.nric.org> (follow “Meetings” to “Friday, December 16, 2005”) at 59 (2005).

supplemented by mobile generators and fuel trucks. The prevailing flexible, best-practices approach to backup power should be updated by industry stakeholders, if necessary, and extended to broadband networks.

The Commission should avoid any prescriptive rules that would impede carriers' necessary flexibility in preparing for and responding to disasters, thus interfering with the Commission's policy of ensuring the resiliency of critical communications networks. The Commission should not attempt to re-impose the *Katrina Order's* specific requirements of a minimum of 24 hours of backup power for central office assets and eight hours for other locations, such as cell sites, remote switches, and digital loop carrier system remote terminals (DLCs). Although the Commission took into account that battery capacity diminishes upon installation and introduced some flexibility to those standards in its *Reconsideration Order*⁶ by focusing on the design of the power sources and whether the provider regularly checks and replaces those sources, that rule-based approach would still impose considerable burdens on providers, while diverting their attention and resources from more effective and less costly ways to protect their networks.

Substantial burdens from these or similar rules would arise even when nearly all of Verizon's assets have power sources that were designed with the backup power capacity set forth in the Commission's prior rule. In fact, all of Verizon's central offices have been engineered to have both battery reserves and generators with 72-hour fuel reserves – i.e., three times the previously mandated capacity. Similarly, all of Verizon's

⁶ See *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Order on Reconsideration, 22 FCC Rcd 18013 (2007) (“*Reconsideration Order*”).

remote switches and DLCs have batteries designed to an eight hour engineering standard and/or on-site generators capable of providing at least eight hours of power. Nearly all of Verizon's cell sites have eight hours of backup power. Certain sites do not because of engineering design trade-offs that consider the criticality of the site, what equipment is installed at the site, neighboring site capacity and coverage overlap, availability of generator or other backup commercial power, and environmental (e.g., space, weight, ventilation, landlord) concerns.

While it would be difficult enough for providers to revisit those engineering decisions and ensure that every key asset had the mandated *designed* backup power, the Commission's prior requirement that *each* asset be "regularly checked" would impose a far greater burden on providers. Although Verizon performs checks on these assets – both in response to alarms and proactively – it is unclear whether the frequency of all its checks would meet that vague "regularly" standard. Verizon typically checks its central office power sources on a monthly basis, and these systems are periodically tested by commercial power failures. But Verizon has approximately **BEGIN CONFIDENTIAL**
END CONFIDENTIAL remote switches and **BEGIN CONFIDENTIAL**
END CONFIDENTIAL DLCs. Given that the actual life of the battery serving those remote switches and DLCs depends on numerous factors and may not, in practice, amount to eight hours of available power at any particular moment in time, Verizon could conceivably be required – on a far more frequent basis than it does today – to assess current levels of backup power; plan for the installation of new equipment; deploy the additional equipment; and resolve regulatory impediments, such as zoning and environmental regulations, that may inhibit its ability to add additional resources to those

facilities. Even if a semi-annual check of each asset were sufficient, Verizon would have to complete these steps for **BEGIN CONFIDENTIAL** **END CONFIDENTIAL** assets *per day*. These efforts would consume a substantial amount of time and effort and would require the acquisition of significant resources, which would otherwise be available to devote to other disaster-planning initiatives or customer-benefitting network improvements and deployment.

Devoting these substantial resources to backup power assessments for DLCs makes even less sense today. When the *Katrina Order* was released, the marketplace was far different, and legacy voice networks served many more customers. Today, customers are steadily being migrated off DLCs as a result of increased adoption of FiOS voice services (which do not utilize DLCs or similarly powered remote assets), cord-cutting, and increased competition from cable competitors that offer interconnected VoIP services. Yet even though these DLCs service fewer and fewer customers, Verizon would still be required by the prior rule to meet a rigorous schedule to assess each and every site. A more flexible approach, such as best practices, would allow Verizon to tailor its assessments to focus on those sites that serve the most customers or may be situated in areas more prone to disasters that require backup power.

In any event, even though the rules from the *Katrina Order* never went into effect, Verizon has been proactively taking measures over the past four years to improve its ability to supply backup power during a disaster. For example, from the date of the *Katrina Order* until the end of 2008, Verizon increased the percentage of cell sites with installed generators by over **BEGIN CONFIDENTIAL** **END CONFIDENTIAL**. Fourteen of Verizon's 20 regions had percentages of **BEGIN CONFIDENTIAL**

END CONFIDENTIAL or greater prior to Verizon's acquisition of Alltel in 2009, which caused a slight decrease in that percentage. Verizon has steadily improved that percentage since then.

Moreover, Verizon has taken substantial steps to improve the energy efficiency of its facilities, from switches to cell sites. In fact, Verizon is seeking Energy Star certifications for various facilities. Improving a facility's energy efficiency will reduce the electrical load that has to be backed up on batteries or generators. Furthermore, Verizon has begun exploring alternative energy sources for primary and/or backup power, such as solar, wind power, and fuel cell technologies. Although all these alternatives have not yet demonstrated the necessary reliability, Verizon is continuing this effort to use the energy sources of tomorrow.

V. The Commission Should Focus on Educating Broadband Customers.

In addition to promoting the establishment and adoption of best practices among providers, the Commission has a role to play in ensuring that broadband customers take appropriate steps to enhance their ability to communicate in the event of network congestion or outage. For example, there are a wide range of activities that end users can undertake to prepare for and help mitigate the effect of a network-affecting event, ranging from limiting broadband use to off-peak time periods to obtaining information from alternative sources, such as broadcast television or radio. In the enterprise space, businesses, too, should take steps to establish alternative means of communications; purchase diverse services for mission critical sites or applications; consider maintaining duplicate "hot sites" from which key data and applications can be accessed in the event of an outage at the primary site; and other such measures.

CONCLUSION

To meet its customers' expectations in the highly competitive marketplace, Verizon has engineered its broadband networks to be available or promptly restored during disasters and severe overloads. The Commission should encourage industry stakeholders to establish and/or update best practices, including those pertaining to backup power, to better prepare for disasters.

Respectfully submitted,

/s/ Mark J. Montano

Michael E. Glover
Of Counsel

Edward Shakin
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3158

John T. Scott, III
Andre J. Lachance
VERIZON WIRELESS
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 589-3740

*Attorneys for Verizon
and Verizon Wireless*

July 7, 2011