

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

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

**COMMENTS OF 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 – recently estimated around \$17 billion – to build, maintain, and protect the health of its networks.<sup>1</sup> 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.”<sup>2</sup>

As described in these comments, Verizon’s 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

---

<sup>1</sup> See Ivan Seidenberg, Defense Information Systems Agency (DISA) Customer Partnership Conference Keynote Address, [http://www22.verizon.com/Content/ExecutiveCenter/Ivan\\_Seidenberg/defense\\_informati\\_on\\_systems/](http://www22.verizon.com/Content/ExecutiveCenter/Ivan_Seidenberg/defense_informati_on_systems/) (last visited June 23, 2010).

<sup>2</sup> *Id.*

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 to ensure that *all* broadband providers have the most effective tools to protect their networks and to ensure that end users take steps where possible to address their specific communications needs.

## **DISCUSSION**

### **I. Verizon's Broadband Networks Have Features That Enhance Survivability.**

Throughout its history of providing communications services, Verizon has faced the risks of natural or man-made disasters and has constructed its network knowing that it was important that the network continue to function despite the existence of such disasters. Verizon well understands the need for customers to have communications available and acts promptly to restore service in the event of an outage. Drawing from this experience as a provider of reliable voice services, Verizon deployed its broadband networks to minimize the risks that the network would not be available. Verizon's extensive experience, ranging from local storms to the terrorist attacks of 9/11, has enabled it to hone its processes and safeguards to better withstand future events. The key processes and safeguards that Verizon employs are discussed below.<sup>3</sup>

First, Verizon sets an internal goal for the availability of its wireline and wireless broadband networks that is similar to its goal for its voice networks. That is, Verizon

---

<sup>3</sup> The descriptions are at a relatively high level to avoid providing wrongdoers with a roadmap that would allow them to circumvent Verizon's protective measures.

endeavors to maintain greater than 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.

Second, Verizon’s broadband networks are 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 LATA core router to the gateway router. Verizon utilizes two circuits in diverse pathways and houses the LATA core 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 Network Operations Centers (NOCs) closely monitor 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 back-up circuits, diverse entrance facilities at the customer premise, and physically diverse routing options, to ensure that such customers can purchase diverse circuits to meet their needs.

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. Furthermore, Verizon's 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. Verizon has mobile assets, such as Cell On Wheels (COW) and Cell On Light Truck (COLT), that it can deploy when additional capacity is required.

The benefits of Verizon's network redundancy and its efforts to manage capacity were illustrated by the record-breaking snowstorms along the East Coast during February 2010. The snowstorms caused residential utilization peaks to shift from evening to

daytime hours because many people worked from home. Verizon effectively managed this shift, and Verizon's wireline broadband consumers were largely unaffected if they retained electric power. The snowstorms did not result in widespread unavailability or systemic congestion. Similarly, while Verizon observed heavy wireless use in suburban neighborhoods, the snowstorms had little effect on Verizon's wireless 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 traffic in real-time and tuned the network by adjusting the footprint of neighboring cell sites to pick up traffic from sites with surges of use. As a result, Verizon experienced a normal day's performance metrics on Inauguration day.

Third, Verizon employs internal physical security practices, including fences, access control systems, alarms, and video surveillance, to guard its critical wireline and wireless network infrastructure. As with other components of the network, the standards to protect Verizon's voice network were used to help develop physical safeguards employed for Verizon's wireline broadband network (which are often located in shared facilities). Buildings are constructed to mitigate risks of natural disasters that are pertinent to the areas in which the buildings are located (e.g., floods, earthquakes, hurricanes, etc.). Moreover, Verizon typically maintains battery back-up in local backbone sites (e.g., central offices) and in Internet backbone sites. In these sites, Verizon also employs fully independent back-up generator systems. In the wireless network, Verizon's mobile switching centers and the vast majority of its cell sites have alternate power supplies via battery backup and generators.

## **II. Verizon Already Works Closely With the Federal Government During Disasters.**

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 National Coordinating Center for Telecommunications (NCC), a 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 an employee 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 partnership with the Department of Homeland Security and the sector-specific federal agencies or SSAs.

In light of the already-established government resources devoted to understanding the availability of broadband networks during disasters, the Commission should continue to focus on establishing and updating best practices that providers can adopt to better protect their broadband networks. Recently, the Commission took an

important step towards that end when it re-chartered the Communications Security, Reliability, and Interoperability Council (CSRIC). The CSRIC is 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. 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.

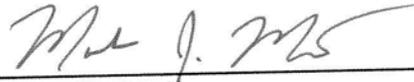
Historical experience demonstrates the success of voluntary best practices. From 2004 through 2006, Verizon participated on the Network Reliability and Interoperability Council (NRIC VII) subcommittee on cybersecurity. The NRIC subcommittee created a report that documented over 200 best practices related 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 numerous 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 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.

In addition to focusing on establishing 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. Because the federal government is already engaged in coordinating the impact of disasters on broadband networks, the Commission should focus on establishing and updating best practices that the industry can adopt to better protect their broadband networks and on educating end users on how to plan for their own communications needs.

Respectfully submitted,



---

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

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

*Attorneys for Verizon  
and Verizon Wireless*

Michael E. Glover  
*Of Counsel*

June 25, 2010