

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

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
THE UNITED STATES TELECOM ASSOCIATION**

Jonathan Banks
Robert Mayer
Kevin G. Rupy
United States Telecom Association
607 14th Street, N.W.
Suite 400
Washington, D.C. 20005
(202) 326-7200

June 25, 2010

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY..... 1

II. PUBLIC-PRIVATE PARTNERSHIPS, NOT INDEPENDENT RULEMAKING, ARE BETTER SUITED TO ENSURING ENHANCED NETWORK RESILIENCY..... 2

III. NETWORK PROVIDERS TAKE SUBSTANTIAL STEPS TO ENSURE RESILIENCY IN THEIR NETWORKS..... 10

A. THE COMMISSION SEEKS SENSITIVE INFORMATION REGARDING NETWORK INFRASTRUCTURE VULNERABILITIES THAT SHOULD NOT BE DISCLOSED IN A PUBLIC PROCEEDING 10

B. CONSISTENT WITH FEDERAL GOVERNMENT PRIORITIES, BROADBAND PROVIDERS ARE INCREASINGLY FOCUSED ON RESILIENCY IN BROADBAND NETWORKS 13

C. BROADBAND PROVIDERS ARE ENGINEERING AND DEPLOYING INCREASINGLY RESILIENT NETWORKS..... 15

IV. NETWORK PROVIDERS ENSURE SUFFICIENT REDUNDANCY IN THEIR NETWORKS..... 16

V. NETWORK PROVIDERS ARE ADEQUATELY ADDRESSING THE RARE INSTANCES OF SEVERE OVERLOADS ON THE NETWORK..... 20

VI. CONCLUSION. 22

* * *

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

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
THE UNITED STATES TELECOM ASSOCIATION**

I. INTRODUCTION AND SUMMARY

The United States Telecom Association (USTelecom) is pleased to provide these comments in the above referenced proceeding, regarding the importance of broadband survivability to consumers, businesses, emergency responders, and government agencies.¹ Consistent with the demands of the current broadband marketplace, USTelecom members place an extremely high value on the security and reliability of their service, networks, and facilities. Whether large or small, they invest heavily in disaster-recovery planning to ensure that their business and residential customers enjoy uninterrupted service of the highest quality. The significant efforts by USTelecom's members have resulted in the deployment of a remarkably robust, secure and survivable broadband network that has performed exceedingly well during times of public emergencies and major catastrophes.

These efforts to further network resiliency have been aided and enhanced by participation in numerous public-private partnerships. These substantial and well-established public-private

¹ Notice of Inquiry, *Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, PS Docket No. 10-92, 25 FCC Rcd 4333 (PS 2010) (*Notice*).

efforts are better suited than independent rulemakings at identifying and addressing network survivability issues on an ongoing basis.

Independently and as a part of these collaborative efforts, network providers continue to take substantial efforts to ensure resiliency in their networks. Broadband providers have voluntarily spent hundreds of millions of dollars ensuring their networks are survivable and resilient. While a detailed accounting of vulnerability issues in a public proceeding runs counter to sound public policy, it is worth noting that carriers implement numerous mechanisms to ensure network survivability that include a combination of sound engineering and adherence to best practices.

Moreover, network providers continue to take substantial steps to ensure sufficient redundancy in their networks. Rather than provide ubiquitous redundancy for each and every network element, broadband providers today have developed a densely connected network that better enables network operators to work around regional or localized disruptions. Occurrences of severe overloads on the network are rare, due to broadband providers' ongoing and evolving efforts to address such instances.

II. PUBLIC-PRIVATE PARTNERSHIPS, NOT INDEPENDENT RULEMAKING, ARE BETTER SUITED TO ENSURING ENHANCED NETWORK RESILIENCY

USTelecom member companies strive to ensure that their residential and business customers enjoy uninterrupted service of the highest quality. They strongly believe in supporting a highly reliable critical infrastructure capable of providing consumers with emergency services in times of national emergency, local disaster, and public health crises. In exploring potential

measures to reduce network vulnerabilities, the Commission should favor public-private partnerships over regulatory intervention.

Regardless of whether the Commission has sufficient statutory authority to exercise its authority over such matters,² a regulatory approach to network survivability ignores the substantial success that has been achieved through existing public-private partnerships that are more ideally suited to achieving the Commission's desired outcomes. Through participation in such public-private partnerships, the Commission can better engage government and industry stakeholders in identifying areas of mutual concern and formulating appropriate solutions that evolve with changes in technology. Indeed, many of the questions posed by the Commission in its current inquiry have been the subject of exhaustive and collaborative public-private partnership inquiries in recent years, and have produced tangible and positive results.³

There currently exists a robust and successful public-private mechanism that is effectively addressing network survivability issues. These joint efforts focus on a broad range of issues, to include incident management, emergency preparedness and risk assessments. Such proactive measures are effectively preventing, addressing and responding to incidents that can feasibly impact the survivability and resiliency of broadband networks. While the Commission

² USTelecom's comments will not address the legal authority issues raised in the Notice. *See, Notice*, ¶¶ 8-9. In light of the Commission's Notice of Inquiry regarding Title II authority, issues relating to the scope of the FCC's authority in such areas are best addressed in that proceeding. *See, Notice of Inquiry, Framework for Broadband Internet Service*, GN Docket No. 10-27, FCC 10-114 (2010).

³ *See e.g.*, Department of Homeland Security Report, *National Sector Risk Assessments Result Report*, April 2008 (*National Sector Assessment Report*); *see also*, National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Physical Assurance of the Core*, November 6, 2008 (*NSTAC Core Report*); DHS Report, *Information Technology Baseline Risk Assessment*, August 2009 (*DHS IT Risk Assessment Report*). Both the *National Sector Assessment Report* and the *NSTAC Core Report* are categorized as "For Official Use Only" and therefore contain information that may be exempt from public release from the Freedom of Information Act.

should not seek to duplicate existing efforts, USTelecom encourages it to become actively engaged in these forums as one of the many expert agencies in this arena.

For example, USTelecom and its largest members are members of the National Coordinating Center (NCC), which operates under the auspices of the National Communications Systems (NCS), Department of Homeland Security (DHS). The NCC was formed in 1984 after the President's National Security Telecommunications Advisory Committee (NSTAC) recommended that a joint industry and government center be formed to coordinate national security and emergency preparedness (NS/EP) telecommunications services. This public-private partnership ensures the timely delivery of resources and technologies to restore critical communications services following an emergency. In addition to the NCC, USTelecom and many USTelecom members are members of the Telecom-Information Sharing and Analysis Center (Telecom-ISAC). The Telecom-ISAC was formed in 2000, when the telecommunications industry partnered with the federal government in response to growing concerns about the physical and cyber vulnerabilities of the nation's telecommunications networks.

Members of the Telecom-ISAC voluntarily share information on physical and cyber vulnerabilities and threats and intrusions to the telecommunications network infrastructure to support reliability and security of the nation's communications networks. The NCC and the Telecom-ISAC have been successful because of industry's willingness to lead the mission of securing and restoring NS/EP communications. Finally, it was USTelecom members, through NSTAC and the NCC, that developed critical NS/EP initiatives, such as the Telecommunications Service Priority (TSP) and Government Emergency Telecommunications Services (GETS),

which, as discussed in more detail below, support their mission-critical communications needs and functions.

In addition to participating in the NCC and Telecom-ISAC, USTelecom members voluntarily participate in development of and compliance with industry best practices regarding reliability and redundancy of networks published by the Commission's Network Reliability and Interoperability Councils (NRIC).⁴ The Commission has convened NRIC on several occasions, including in 2003 (NRIC VI), when it was convened to consider and adopt best practices aimed at improving "the reliability, robustness, security, and interoperability of public telecommunications networks."⁵ To fulfill this mandate, NRIC VI established focus groups to examine the areas of network reliability, network interoperability, broadband, and homeland security. The homeland security group examined physical and cyber security, public safety, disaster recovery and mutual aid, and developed physical and cyber security best practices to prevent, restore and recover the nation's telecommunications networks from future disasters or attacks.⁶

This group developed physical security restoration and prevention best practices across all segments of the communications industry in an "all hazards" approach. These best practices address not just hurricanes, but other hazards such as floods, fires, tornadoes, winter storms,

⁴ NRIC was established by the FCC in 1992 and for the last several years, this industry-led initiative has been developing best practices to reduce outages and improve communications for the nation.

⁵ See NRIC website, *Charter of the Network Reliability and Interoperability Council - VI* (http://www.nric.org/charter_vi/index.html) (visited June 24, 2010).

⁶ The homeland security group assessed the "vulnerabilities of the communications infrastructure" and determined "how best to address those vulnerabilities to prevent, minimize, or restore from, disruptions that could result from terrorist activities, natural disasters, or similar types of occurrences." Final Report, *Network Reliability and Interoperability Council VI, Homeland Security, Physical Security, Focus Group 1a*, p. 7, December 3, 2003 (available at: <http://www.nric.org/fg/nricvifg.html>) (visited June 24, 2010).

chemical and biological spills, and pandemics. USTelecom members apply this “all hazards” approach in their business continuity plans and disaster recovery efforts as appropriate.

The Commission has since renewed the charter for the Communications Security, Reliability, and Interoperability Council (CSRIC).⁷ The purpose of the CSRIC is to provide recommendations to the Commission to ensure optimal security, reliability, operability and interoperability of communications systems, including public safety, telecommunications, and media communications systems. In this regard, the Commission established Working Group 6 of the CSRIC (Best Practice Implementation). Working Group 6 is currently working to develop options and recommendations for CSRIC’s consideration regarding the key best practices for communications service providers to implement in order to enhance the security, reliability, operability and resiliency of communications infrastructure.⁸ These ongoing public-private efforts are generating tangible results that will further the efforts of industry and government to identify and prioritize the most critical best practices for communications providers to adopt and implement.

In addition, the DHS, whose mission includes “preparation for and response to all hazards and disasters,”⁹ recently commended the substantial benefits resulting from public-private partnerships in the information technology (IT) sector.¹⁰ In particular, DHS highlighted the fact that “public and private sector partners bring unique capabilities to the partnership and

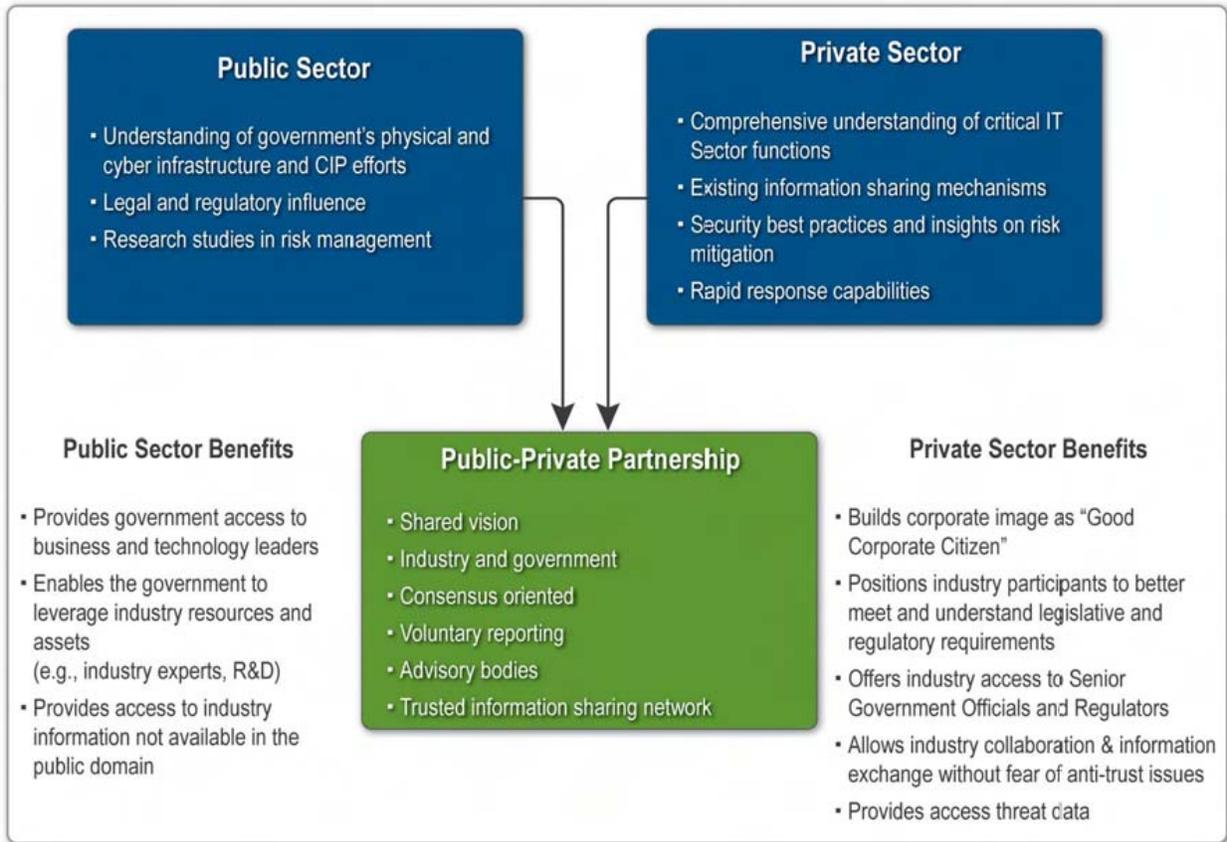
⁷ See, Public Notice, *FCC Seeks Nominations by May 11, 2009 for Membership on the Communications Security, Reliability, and Interoperability Council (CSRIC)*, DA 09-816, 24 FCC Rcd 4201 (2009).

⁸ See, CSRIC website, *CSRIC Working Group Descriptions, Working Group 6 – Best Practice Implementation* (available at: <http://www.fcc.gov/pshs/advisory/csric/wg-6.pdf>) (visited June 25, 2010).

⁹ See DHS website, *Strategic Plan — One Team, One Mission, Securing Our Homeland* (available at: <http://www.dhs.gov/xabout/strategicplan/>) (visited June 15, 2010).

¹⁰ See, *DHS IT Risk Assessment Report* (available at: http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf) (visited June 15, 2010).

derive unique benefits through public-private sector collaboration.”¹¹ The virtuous cycle resulting from such public-private partnerships – and the benefits for both public and private entities – is reflected in the below diagram:¹²



In discussing the IT Sector-Specific Plan (SSP), which includes broadband providers, DHS referred to the public-private partnership as “an unprecedented partnership and collaboration between public and private sectors as they leverage their unique capabilities to address the complex challenges of IT infrastructure protection.”¹³ USTelecom expounded at

¹¹ *DHS IT Risk Assessment Report*, p. 10.

¹² *Id.*

¹³ *Id.*

length on the many tangible and positive results resulting from such public-private partnerships in the Commission's National Broadband Proceeding last year.¹⁴

In addition, the DHS currently coordinates the efforts of the Critical Infrastructure Partnership Advisory Council (CIPAC).¹⁵ The CIPAC facilitates effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments. The CIPAC represents a strong partnership between government and critical infrastructure/key resource (CIKR) owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.

An additional forum for the Commission to become engaged is through the National Infrastructure Protection Plan (NIPP) and its 18 supporting Sector-Specific Plans (SSPs) under the auspices of the DHS. As former Secretary Michael Chertoff noted in the preface to the most recent NIPP, the partnership "has been a major accomplishment to date and has facilitated closer cooperation and a trusted relationship in and across the 18 [critical infrastructure and key resources] sectors."¹⁶ Secretary Chertoff went on to note that [t]his multidimensional public-private sector partnership is the key to success in this inherently complex mission area," and is the "path to successfully enhancing our Nation's CIKR protection."¹⁷

¹⁴ See Comments of USTelecom, November 12, 2009, pp. 2-19; submitted in response to, Public Notice, *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice # 8, DA 09-2133 (released September 28, 2009).

¹⁵ See, DHS website, *Critical Infrastructure Partnership Advisory Council* (available at: http://www.dhs.gov/files/committees/editorial_0843.shtm) (visited June 14, 2010).

¹⁶ See, DHS Report, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency*, 2009, Preface (available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) (visited June 22, 2010) (*NIPP*).

¹⁷ *Id.*

As the key regulator over one of the components of the network infrastructure environment, this type of participation is well suited for the Commission, which can complement existing coordination efforts by other critical agencies. Participation in the implementation of the NIPP provides the government and the private sector with the opportunity to use collective expertise and experience to more clearly define CIKR protection issues and practical solutions and to ensure that existing CIKR protection planning efforts, including business continuity and resiliency planning, are recognized.

The Commission should also consider outreach efforts to consumers and industry to ensure effective practices with respect to network survivability. Such an approach is consistent with the Chairman's September 2009 30 Day Review of FCC Preparedness for Major Public Emergencies.¹⁸ In that document, the Chairman concluded that while the FCC has shown it is prepared to respond to communications emergencies and perform its mission, among the areas in which emergency planning and response could be improved was expansion of "public safety and emergency response outreach activities."¹⁹ The 30 Day Review lists numerous areas for such outreach.²⁰

¹⁸ FCC Report, *FCC Preparedness for Major Public Emergencies, Chairman's 30 Day Review*, September, 2009 (available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf) (visited June 22, 2010) (*Chairman's 30 Day Review*).

¹⁹ *Id.*, p. 3.

²⁰ Among other things, the Chairman's 30 Day Review recommends expansion of public safety and emergency response outreach activities (*Chairman's 30 Day Review*, p. 3); outreach efforts directed at incumbent LECs, competitive LECs, and other providers during emergencies (*Id.*, p. 9); outreach by Public Safety and Homeland Security Bureau (PSHSB) personnel to public safety entities, and outreach by other Bureau personnel to FCC licensees (*Id.*, p. 19); outreach to entities not engaged in the NRIC process, in order to "expand awareness and encourage implementation of NRIC best practices," (*Id.*, p. 28); and deployment of a new Emergency Operations Outreach Specialist who would "establish working relationships with and the support of public safety officials before incidents occur" (*Id.*, p. 32). In addition, the PSHSB has compiled "a comprehensive outreach program that serves law enforcement, fire fighters, emergency medical technicians, 911 call centers, health care facilities and the

Additional outreach, particularly to the consumer and small business communities, can be coordinated through the Commission's Consumer and Governmental Affairs Bureau (CGB). The CGB has a long track record of successful outreach in this area, and is well suited for informing consumers and small businesses about critical issues in the network survivability context.²¹

III. NETWORK PROVIDERS TAKE SUBSTANTIAL STEPS TO ENSURE RESILIENCY IN THEIR NETWORKS

Network providers continue to engineer robust resiliency mechanisms and procedures into their broadband networks. Over time, and through intense communications facilitated through existing public-private partnerships, these measures continue to evolve and mature. Such sensitive critical infrastructure information should not be divulged in a public proceeding. Placement into the public record of sensitive information regarding the vulnerabilities, risks and survivability features of broadband networks ignores well-established practices by other Federal agencies with an equal stake in consideration of these issues.

A. The Commission Seeks Sensitive Information Regarding Network Infrastructure Vulnerabilities that Should Not Be Disclosed in a Public Proceeding

In its notice, the Commission seeks extremely sensitive information regarding the survivability features and risks presented by the physical architecture of current broadband

communications sector." The robust efforts of the PSHSB in this regard are detailed in a published report. *See*, PSHSB website, *PSHSB Outreach* (available at: <http://www.fcc.gov/pshs/docs/outreach.pdf>) (visited June 23, 2010).

²¹ The CGB has conducted extensive outreach in several critical areas, including the Rural Health Care Pilot Program, Lifeline and Link-Up, the Do-Not-Call Registry and the digital television transition (*see* CGB website, available at: <http://www.fcc.gov/cgb/>) (visited June 22, 2010).

communications networks.²² USTelecom believes it would be ill-advised to place such sensitive information into a public record. Among other things, the Commission seeks detailed analysis of where network specific vulnerabilities reside and how network providers address vulnerability concerns. Placing such information in the public record ignores well-established practices by other Federal agencies with an equal stake in consideration of these issues.²³

Sensitive treatment of information pertaining to critical infrastructure resources not only constitutes sound public policy, but is also dictated by statute and governed by Presidential Directive. For example, the Critical Infrastructure Information Act of 2002 (CIIA) addresses the circumstances under which the DHS may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program.²⁴ It establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS. The CIIA was enacted to address the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets.

Similarly, DHS Presidential Directive 7 (DHS-PD-7) establishes a national policy for Federal departments and agencies to prioritize critical infrastructure and to protect it from

²² Notice, ¶¶ 10-12. Among other things, the FCC seeks comment on “major single points of failure in broadband architectures,” measures taken by communications providers “to minimize the presence of single points of failure in broadband architectures,” identification of the “most effective” and “widely deployed” NRIC physical security best practices and whether the present level of protection is “adequate.”

²³ See, Report and Order and Further Notice of Proposed Rulemaking, *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ¶¶, 45 - 46, 19 FCC Rcd. 16830, 69 FR 68859 (2004).

²⁴ See, 6 U.S.C. § 131 et seq.

terrorist attacks.²⁵ As an independent agency of the United States Government,²⁶ the Commission is required under DHS-PD-7 to “appropriately protect information . . . that would facilitate terrorist targeting of critical infrastructure and key resources.”²⁷ Placement of such sensitive information into a publicly available record runs counter to this Executive Branch guidance.

The DHS’s most recent NIPP notes that sensitive information relating to critical infrastructure assets “could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information.”²⁸ After noting that the Federal Government has a “statutory responsibility to safeguard information collected from or about CIKR activities,”²⁹ it goes on to catalogue an exhaustive list of mechanisms it uses to ensure security of this information.³⁰ Indeed, the DHS includes as one of its responsibilities in establishing a NIPP the “protect[ion] [of] sensitive information voluntarily provided by the private sector.”³¹

Moreover, in recent years the DHS has expressed these national security concerns to the Commission. For example, when the Commission was first considering outage reporting requirements, the DHS expressed its view that any outage reporting requirements adopted by the Commission “must be accompanied by appropriate measures to safeguard reporting data to the

²⁵ See DHS website, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (available at: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm) (visited June 22, 2010) (*Presidential Directive #7*).

²⁶ See, 5 U.S.C. §104(1).

²⁷ See, *Presidential Directive #7*, ¶10.

²⁸ See, *NIPP*, p. 66.

²⁹ *NIPP*, p. 66.

³⁰ *Id.*, pp. 66 – 69.

³¹ *Id.*, p. 17.

maximum extent consistent with applicable information access laws.”³² DHS went on to note that while the information is critical to identifying and mitigating vulnerabilities in the system, “it can equally be employed by hostile actors to identify vulnerabilities for the purpose of exploiting them.”³³

B. Consistent with Federal Government Priorities, Broadband Providers Are Increasingly Focused on Resiliency in Broadband Networks

While the Commission proceeding appropriately considers threats and potential gaps affecting the survivability and protection of broadband networks, this is only one piece of the equation. As Commissioner Baker noted in her statement accompanying this notice, the Commission “should be careful not to fix ourselves [to] every challenge that relates in some form to broadband.”³⁴ Rather, in recent years efforts have been increasingly focused on a strategy that “appropriately balances resiliency . . . with focused, risk-informed prevention, protection, and preparedness activities.”³⁵

The DHS’s most recent NIPP places a greater emphasis on the concept of resiliency, which is the capability to resist, respond to and recover from disasters. In particular, the 2009 version of the plan discusses resiliency with the same level of importance as protection, whereas an earlier version treated resiliency as a subset of protection.

³² See, Comments of the DHS, June 2, 2004, p. 14, submitted in response to, Notice of Proposed Rulemaking, *New Part 4 of the Commission’s Rules Concerning Disruptions to Communications*, 69 Fed. Reg. 15761, ED Docket No. 04-35 (2004) (*DHS Outage Reporting Comments*).

³³ *Id.*, p. 14.

³⁴ See, Notice, Statement of Commissioner Meredith Attwell Baker.

³⁵ *NIPP*, Preface.

The most recent SPP, published by the DHS in February of 2009, addressed the effectiveness of engineered resiliency within communications networks. That report concluded that while the events of September 11, 2001, and the hurricanes of 2005 “highlighted the importance of communications to public health and safety, to the economy, and to public confidence,” these disasters “proved the overall resiliency of the national communications network.”³⁶ The report noted that “[d]espite the enormity of these incidents, the network backbone remained intact.”³⁷ Further buttressing this point, a recent report from the Government Accountability Office found that while the discussion of resiliency in some SSPs was somewhat limited, discussion of resiliency in the communications SSP was “relatively extensive.”³⁸

In a similar vein, the DHS’s most recent NIPP noted that “[i]n situations where robustness and resiliency are keys to CIKR protection, providing protection at the system level rather than at the individual asset level may be more effective and efficient.”³⁹ So, for example, where there are many similar facilities, it may be optimal to allow other facilities to provide the infrastructure service rather than to deploy limited resources to protect each and every facility.

³⁶ See, DHS Report, *Communications, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan*, p. 5, May 2007 (available at: <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf>) (visited June 22, 2010) (*Communications SSP*).

³⁷ *Id.*

³⁸ GAO Report, *Critical Infrastructure Protection, Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296, pp. 24-25, March 2010.

³⁹ *NIPP*, p. 43.

C. Broadband Providers Are Engineering and Deploying Increasingly Resilient Networks

USTelecom member companies have voluntarily spent hundreds of millions of dollars and countless hours preparing for disaster recovery.⁴⁰ They have made these preparations in order to ensure continued quality service to their customers, even in times of dire emergency. Ensuring their ability to maintain high quality, uninterrupted service is of paramount importance to USTelecom members and is a huge incentive for them to continue participating in industry groups focusing on network reliability and disaster preparedness, in the development of industry best practices, and in refining business continuity plans.

With more than 85 percent of the nation's critical infrastructure owned and operated by private companies,⁴¹ there are substantial market-based incentives to invest in and secure critical communications infrastructure. These critical investments by network operators not only ensure redundancy within the network, but also ensure the implementation of robust practices and processes that allow these businesses to react more rapidly during times of crisis, thereby ensuring the viability and survivability of the network.

Network providers take a wide variety of steps and precautions to minimize impacts that could result from any event that could adversely impact network survivability. In the broadest sense, network providers apply the NRIC best practices as appropriate in their networks.

Voluntary adoption and use of these best practices is widespread throughout the industry and has

⁴⁰ See Comments of USTelecom, August 7, 2006, pp. 4 - 9; submitted in response to, Notice of Proposed Rulemaking, *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, 21 FCC Rcd 7320, EB Docket No. 06-119 (2006).

⁴¹ Rep. Bart Gordon (D-TN), The Hill, *Cybersecurity is National Security*, July 14, 2009 (available at: <http://science.house.gov/press/PRArticle.aspx?NewsID=2609>) (visited June 25, 2010).

contributed over time to creating one of the most reliable communications infrastructures in the world.

Carriers implement numerous engineering measures to ensure network survivability that include route diversity, ring architectures, and other features that provide redundancy in the design of high capacity circuits, and greater resiliency when underlying network elements experience a failure. Mitigation actions are also taken through effective network management. During an outage, the ability to prioritize or reroute less important traffic to preserve highly critical traffic is crucial.

Regardless of the type of network platform, private companies' business models are fully dependent on having a secure, resilient and reliable network. Flaws in reliable infrastructure result in private companies losing customers and business. As a result, businesses are taking substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace. Such guarantees in level of service are routinely embodied in service level agreements (SLAs) between network providers and enterprise customers. SLAs are of fundamental importance in today's business environment, where an established level of service is formally defined, and network providers are under a contractual obligation to meet their commitments.

IV. NETWORK PROVIDERS ENSURE SUFFICIENT REDUNDANCY IN THEIR NETWORKS.

Network providers take substantial steps to engineer and deploy IP networks that are reliable, redundant and capable of effectively responding to external forces that can damage or degrade their functionality. While no provider can ensure redundancy for every segment of their

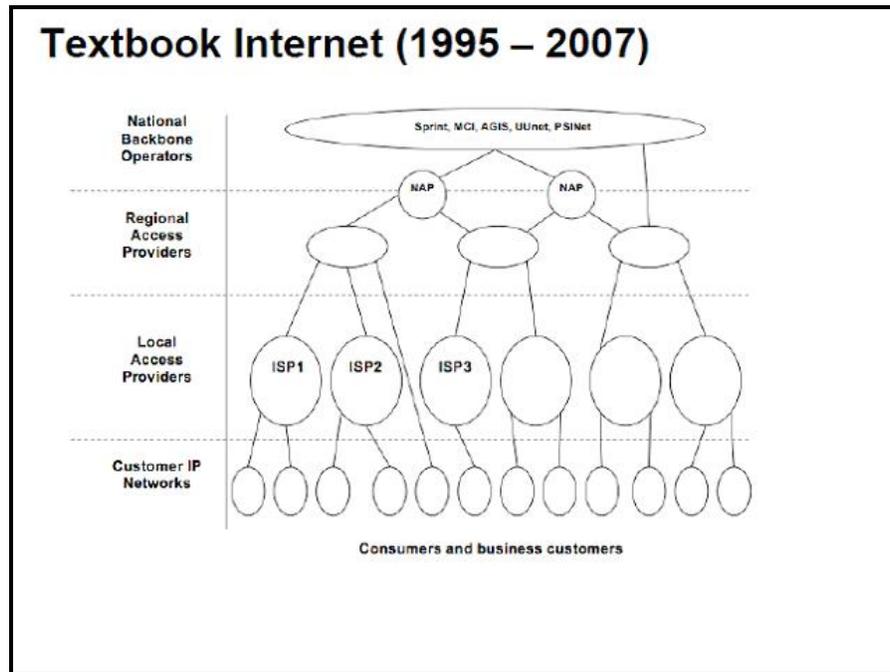
respective broadband network, sufficient redundancy is engineered to ensure that appropriate levels of service are available during instances of extreme traffic.

Of particular importance, today's Internet – particularly at the core – has evolved into a more resilient and redundant network that is better suited to address instances of localized disruptions. The evolution of the Internet core was recently captured in the Annual Report by the ATLAS Internet Observatory (ATLAS Report).⁴² The ATLAS Report's comparison between the Internet of the past, with the "New Internet," demonstrates how the Internet has moved from traditional hierarchical networks to more open architecture.

Pictured below is the ATLAS Report's representation of the so-called "Textbook Internet" of 1995 through 2007.⁴³ Key to this former architecture was the hierarchical nature of the network: online consumers accessed any content on the Internet through a vertical path -- initiating at the ISP, passing over a regional access provider's network and using facilities of a national backbone operator. This mechanism resulted in a form of "out and back" network, where IP traffic was provisioned to the consumer through a similar routing of traffic.

⁴² Annual Report by the ATLAS Internet Observatory, Arbor Networks Inc., University of Michigan, Merit Networks, Inc. (available at: http://www.eecs.umich.edu/eecs/about/articles/2009/Observatory_Report.html) (visited January 11, 2010) (*ATLAS Report*). The ATLAS Report, which details a landmark two-year study of global Internet traffic that offers detailed trend data and analysis, was developed by researchers at the University of Michigan, Arbor Networks, and Merit Network. The ATLAS Report, believed to be the largest study of global Internet traffic since the birth of the commercial Internet in the mid-1990s, provides analysis of two years' worth of detailed traffic statistics, as the study, at its peak, monitored more than 12 terabits per second for a total of more than 256 exabytes of Internet traffic.

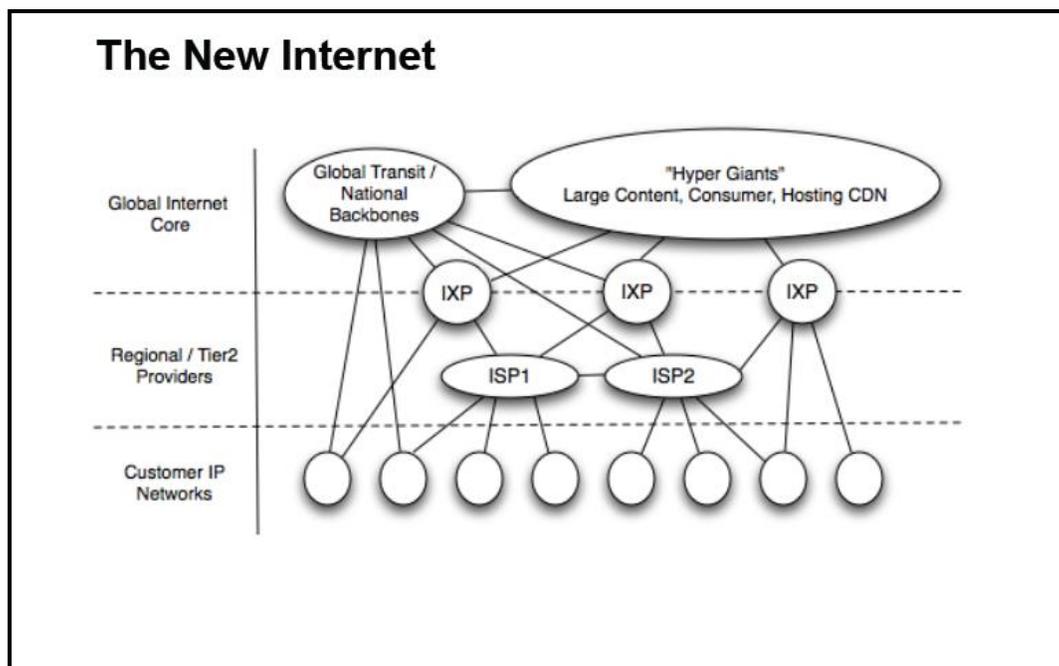
⁴³ This version of the Internet was embodied in four key segments: 1) National Backbone Operators (*e.g.*, Sprint, MCI, UUNet); 2) Regional Access Providers; 3) Local Access Providers (*i.e.*, traditional ISPs); and 4) Customer IP Networks. *ATLAS Report*, p. 9.



But with the innovation and evolution of the Internet ecosystem, Internet architecture has moved from traditional hierarchical networks to more open architecture. As the ATLAS Report highlights, there is today a new core of interconnected content and consumer networks that have resulted in “dramatic improvements in capacity and performance.”⁴⁴ This shift in network design has resulted in tremendous disintermediation; in some instances it has resulted in the direct interconnection between content and consumers. As Danny McPherson, the Vice President and Chief Security Officer of Arbor Networks (one of the contributors to the study), commented, “[t]he Internet is a lot flatter today, more densely connected.”⁴⁵ A reflection of this more robust network is captured in the below diagram from the ATLAS Report.

⁴⁴ *Id.*, p. 17.

⁴⁵ Thomas Claburn, Information Week, *Google Now Largest Source of Internet Traffic*, October 13, 2009 (available at:



The result of this “more densely connected” network is an inherent redundancy throughout the Internet ecosystem that better enables network operators to work around regional or localized disruptions. In addition to being more effective and responsive, such efforts are also transparent to consumers and other stakeholders. In contrast, ubiquitous redundancy would be impossible to implement and would arguably result in a less redundant network, since valuable resources would need to be redirected from other critical efforts.

Finally, while redundancy is primarily an issue to be addressed by individual carriers, consumers are increasingly establishing redundancy on their own. In addition to having a landline/IP based voice service, most consumers also maintain backup communications in the form of wireless voice/data services.

http://www.informationweek.com/news/infrastructure/management/showArticle.jhtml?articleID=220600387&cid=RSSfeed_IWK_All (visited June 22, 2010).

V. NETWORK PROVIDERS ARE ADEQUATELY ADDRESSING THE RARE INSTANCES OF SEVERE OVERLOADS ON THE NETWORK.

There is a tremendous success story in the ability of network providers to respond to dramatic changes in broadband usage patterns, despite the presence of several large scale catastrophes in recent years. Since the events of September 11th, carriers have demonstrated the resiliency and robustness of their broadband networks during such events. The resiliency of carriers' networks has been evident in various regional catastrophes.

Large scale events, such as hurricanes, flooding or severe weather can, cause dramatic changes in broadband usage patterns as traffic that is ordinarily confined within enterprise networks suddenly shifts onto residential-access networks. Yet despite the occurrence of several such events in recent years, there have been few major occurrences of severe overloads on communications networks.⁴⁶

This impressive track record is due in large part to ongoing and evolving efforts of network providers. Many of these measures have been developed by carriers based on their

⁴⁶ For example, during the 2008 hurricane season, 17 storms formed in the Atlantic, of which four hurricanes and three tropical storms threatened and/or made landfall in the United States. According to its 2008 Annual Report, the NCS monitored all of these storms which "had very little impact to the infrastructure." NCS Report, Fiscal Year 2008 Report, p. 8 (available at: http://www.ncs.gov/library/reports/ncs_fy2008b.pdf) (visited June 25, 2010) (*NCS 2008 Annual Report*). Similarly, the impacts on communications networks of Hurricane Dolly were "mitigated due to preparedness level of both the State of Texas and the resilience of the communications infrastructure." *NCS 2008 Annual Report*, p. 8. In addition to natural catastrophes, other events demonstrated the resiliency of the communications network. For example, there were concerns that the 2009 Presidential Inauguration would cause major strains on the network. However, the networks of several major carriers handled "millions of additional calls, texts and downloads without any major incidents or failures." See, Leslie Cauley, *Cell Networks Handle Inauguration Volume Smoothly*, USA Today (available at: http://www.usatoday.com/tech/news/2009-01-20-inauguration-cellphones_N.htm) (visited June 25, 2010). Despite these measures, however, the Commission should set realistic expectations. During large scale events, there is the possibility that broadband users may experience degraded or latency in services for brief periods. As the Commission analyzes comments in this proceeding, it is important that it distinguish between these limited degradations or latencies to services and the potential for broadband service outages. While limited instances of service outages are to be expected during large scale emergencies, short-term degradation or latency to service will likely occur as providers seek to restore service to impacted regions. Communications providers are appropriately focused on keeping their networks up and running during these instances.

years of experience responding to large scale events, as well as through their involvement with various public-private partnerships.

As an initial step, traffic management plays a critical role during large scale emergencies. For example, some network service providers have mechanisms in place to implement rate limits or temporary bandwidth caps in discrete areas. Network management tools can be effective mechanisms for improving traffic flow for all users, and effectively limiting congestion to limited areas of the network. For example, a network service provider might rate limit a certain node so that a surge traffic load does not cause congestion that may propagate to other parts of the network.

In addition, where possible, network service providers engineer their networks to enable remote access capabilities to network equipment during times of emergency. Such mechanisms enable network providers to continue operations, by remotely managing their networks during large scale events. As a result, even in instances where a provider's employees who are critical to business continuity efforts may be unable to physically report to work, they are able to remotely perform their functions. Moreover, such capabilities mean that employees well outside the impacted area can nevertheless conduct vital operations to ensure the continued resiliency of the network.

Cross-training of employees is an additional measure network providers undertake to ensure greater resiliency of their networks. Whether critical employees are unable to conduct normal work activities due to the presence of a major pandemic or physical damage, the ability of personnel to competently conduct additional assigned duties enhances the ability of network providers to respond more effectively to large scale events.

Finally, many network providers have obtained Government Emergency Telecommunications Service (GETS) and/or Wireless Priority Service (WPS) capabilities for employees that are critical to business continuity contingencies. As a result of this designation, these employees have priority service for voice communications during large scale emergencies, thereby enhancing their ability to initiate and complete priority tasks.

In addition to GETS and WPS, USTelecom urges the Commission to promote the use of Telecommunications Service Priority (TSP), which enables a qualifying user to get priority restoration and provisioning of telecommunications services. TSP can be placed on business circuits that are deemed to be critical for national security or emergency preparedness, which can help greatly in prioritizing and restoring critical services. The Commission, in partnership with NCS, should undertake a comprehensive awareness program to educate federal, state, and local authorities and enterprise customers, as appropriate, about the benefits of the GETS/WPS and TSP programs in aiding emergency planning and preparedness efforts.⁴⁷

VI. CONCLUSION.

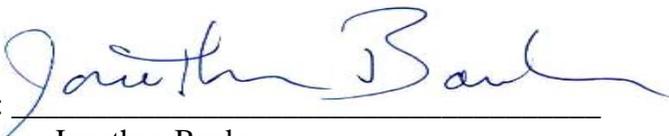
USTelecom members place an extremely high value on the security and reliability of their service, networks, and facilities. These efforts have resulted in the deployment of a remarkably robust, secure and survivable broadband network that has performed exceedingly well during times of public emergencies and major catastrophes. Existing public-private

⁴⁷ For example, the NSC noted in its *NSC 2008 Annual Report*, that “[m]any additional health care facilities now have priority telecommunications programs such as the [TSP] due in large part to the shared effort between [Health and Human Services] and the [Commission].” *NSC 2008 Annual Report*, p. 71.

partnerships have proven to be a robust and effective mechanism for effectively addressing network survivability issues.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: 

Jonathan Banks
Robert Mayer
Kevin Rupy

607 14th Street, NW, Suite 400
Washington, D.C. 20005