Before the
Federal Communications Commission
Washington, D.C.

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

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Andy Scott
Vice President, Engineering

Stephanie B. Power
Research Assistant

Neal M. Goldberg
Loretta Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

June 25, 2010

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY 1

I. TODAY'S BROADBAND COMMUNICATIONS NETWORKS ARE BUILT TO OVERCOME SIGNIFICANT DAMAGE AND THREATS TO THE PHYSICAL INFRASTRUCTURE AND TO WITHSTAND SEVERE OVERLOAD CONDITIONS 4

A. The Cable Broadband Network Possesses Fundamental Architectural Elements and Infrastructure Design to Promote Resiliency and Survivability 6

B. The Performance of Cable Broadband Networks During Recent Natural Disasters Attests to their Resilience and Survivability 11

II. THE EXISTING PUBLIC-PRIVATE PARTNERSHIPS UNDER THE FCC AND DHS AIMED AT PROTECTING BROADBAND COMMUNICATIONS NETWORKS ARE THE BEST APPROACH TO ADDRESSING BROADBAND NETWORK SURVIVABILITY 12

III. THE COMMISSION SHOULD ENCOURAGE A BROAD APPROACH THAT ENCOMPASSES THE VARIED THREATS TO BROADBAND INTERNET COMMUNICATIONS 18

CONCLUSION 19

Before the
Federal Communications Commission
Washington, D.C.

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

COMMENTS OF
THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA") hereby submits its comments in response to the Notice of Inquiry ("NOI") issued by the Commission in the above-captioned proceedings.[1]

INTRODUCTION AND SUMMARY

In this proceeding, the Commission seeks comment on the present state of survivability in broadband communications networks and seeks to explore network vulnerability to failures in equipment or severe overload conditions, such as during natural disasters, pandemics or other emergency situations. In particular, the Commission requests information on "the ability of existing networks to withstand localized or distributed physical damage, including whether there is adequate network redundancy and the extent of survivability of physical enclosures in which network elements are located, and severe overloads."[2]

---

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of high-speed Internet service ("broadband") after investing over $160 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to over 20 million customers.

[2] *In re Effects on Broadband Communications Networks Of Damage to or Failure of Network Equipment or Severe Overload*, Notice of Inquiry, 25 FCC Rcd 4333 ¶ 3 (2010) ("*NOI*").

In recent years, the reliability and resilience of the nation's communications networks in the event of physical harm, severe overload, cyber attacks and other threats to the infrastructure has been given high priority in the federal government, including the White House and the U.S. Department of Homeland Security. In light of this heightened prominence and its past experience with the Network Reliability and Interoperability Council ("NRIC") and Media Security and Reliability Council ("MSRC"), the Commission recently-created the Communications Security, Reliability and Interoperability Council ("CSRIC"), which is providing the platform for refining and developing best practices and other mechanisms to enhance the survivability of 21st century broadband communications.

As discussed below, the cable broadband network physical infrastructure is highly robust and resilient on many fronts – *i.e*. it has "the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions."[3] Redundancy in the network is a key component to avoiding sudden disruptions of Internet traffic flows as a result of disasters, pandemics or other crisis situations, and the modern cable broadband network contains a host of redundancies incorporated into the architecture to prevent service outages, notably redundant fiber rings and optical node receivers. The routing and rerouting of information occurs automatically to avoid congestion and failures in connectivity.

The structural features and capabilities built into cable broadband networks reflect years of risk assessment and analysis and deployment of best practices by network engineers, who constantly improve and upgrade their systems to be responsive to new and emerging threats. And in today's competitive environment, broadband network providers must meet high standards

[3] United States Government Accountability Office, *Critical Infrastructure Protection, Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience* at 4, GAO-10-296 (Mar. 2010) (citing the Department of Homeland Security (DHS) definition of "resiliency") ("*GAO Critical Infrastructure Report*").

of reliability, resiliency and security. It is in their economic interest to design and deploy robust and resilient networks that appeal to residential consumers and commercial users. And they have every incentive to undertake steps to ensure that their network architecture has sufficient redundancy, capacity, and security to withstand physical harm, severe loads, and other stresses to the infrastructure.

But each broadband network has unique characteristics and deploys its own network management techniques to enable the rapid and seamless flow of information. Broadband network operators continually experiment and innovate in order to address the need for ubiquitous reliability to ensure a quality experience for their customers. Moreover, they operate within the vast scope of the inter-connected communications and information systems of the Internet ecosystem. As it looks at survivability issues, the Commission should be mindful that today's broadband communications is characterized by a complex web of entities, including broadband network providers, providing a wide array of interrelated functions. Indeed, given the nature of the threats to Internet communications – which are global in scope and pertain to applications to an even greater degree than to broadband access facilities – the scope of the Commission's inquiry should be commensurately broad.[4]

The federal government has played and continues to play an important role in collaborating with private sector companies to develop methodologies and best practices to protect broadband communications networks. It has promoted policies that allow flexibility and innovation in combating both physical and cyber threats to broadband networks. We believe that the existing public-private framework, in which the Commission plays an active role, is the best

[4] In addition to these comments on survivability of networks and facilities, e.g., servers and other critical components of applications and on-line communication services upon which consumers' rely for Internet communications that may be disrupted in times of natural or man-made disasters, NCTA plans to address cyber security issues – which not only affect the entire Internet ecosystem but may disproportionately affect application providers – in the Commission's parallel proceeding in PS Docket No. 10-93.

means to achieve network survivability goals. This also will promote continuity of federal government structures and strategies aimed at protecting broadband communications in the future. And in this regard, CSRIC will contribute valuable information and recommendations to this ongoing process.

We wish to point out, however, that given the extremely sensitive nature of the information involved here, the Commission should not seek to put this information in the public record. From a public safety and national security perspective, it would be ill-advised given the risk of providing a roadmap to those who wish to harm the nation's broadband communications infrastructure.

I. TODAY'S BROADBAND COMMUNICATIONS NETWORKS ARE BUILT TO OVERCOME SIGNIFICANT DAMAGE AND THREATS TO THE PHYSICAL INFRASTRUCTURE AND TO WITHSTAND SEVERE OVERLOAD CONDITIONS

In the NOI, the Commission recognizes that the network infrastructure required to support the diverse needs of broadband communications – video, voice, data for fixed and mobile use – is extensive and complicated and has led to the development of robust networks with survivability features. It is concerned, however, that these features may not adequately ensure the survivability of all types of broadband service throughout the country. And while presuming that broadband core networks are quite survivable, it asserts that survivability is "generally weaker in segments of communications networks closer to the network edge."[5] It therefore seeks information on the resilience and survivability of our national broadband infrastructure under three broad classes of harm: (1) physical damage (whether due to malevolent acts, accidents or force majeure); (2) inadequate redundancy; and (3) severe network overload.

[5] NOI ¶ 7.

Before addressing the cable broadband infrastructure as it pertains to these potential harms, we wish to note, as an initial matter, that in 2007, the Sector Specific Plan (SSP) developed under the U.S. Department of Homeland Security's National Infrastructure Protection Plan (NIPP) found that communications, as one of the 17 sectors, is *resilient "by design*."[6] In describing the communications sector plan last year, the United States Government Accountability Office (GAO) reported:

> Resiliency is achieved by the technology, redundancy, and diversity employed in network design and by customers who employ diverse and resilient primary and backup communications capabilities, thereby increasing the availability of service to customers and reducing the impact of outages. For example, according to the Communications SSP, the network backbone remained intact on September 11, 2001, and during the hurricanes of 2005 despite the enormity of these incidents.[7]

The SSP further discussed how "the sector mitigates cascading effects of incidents by building resilient communications systems and networks to ensure disruptions remain largely localized and do not affect the national communications backbone."[8] And even in regional and local networks, broadband network operators have designed their networks with substantial redundancies and safeguards that minimize the impact of failures and ensure that their customers continue to receive reliable service.

Thus, the modern broadband communications network is by nature designed to limit and contain harm to promote resilience and survivability at the core *and* at the edge of the network. The overarching design consideration of modern broadband networks is service reliability end-to-end. Very few single points of failure exist in the network, and those are largely localized so

---

[6] United States Dep't of Homeland Security, *Communications Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* at 34, 88 (May 2007) (emphasis added) ("*DHS Communications Sector–Specific Plan*"), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf.

[7] *GAO Critical Infrastructure Report* at 25.

[8] *Id.* at 33.

that any single failure impacts as few customers as possible and can be remedied quickly. When faced with physical damage or severe overload conditions, the network frequently is capable of self-healing through a variety of means, such as dynamic routing (both within backbones and between different ISP backbones); backup and redundant power; and multiple access points to reach fiber and other facilities. While no design is totally fool-proof in the face of unknown catastrophic events, broadband networks are able in most instances to manage such conditions in a manner that maintains quality and is transparent to the end user. The performance of these networks during the record-breaking snowstorms and floods of the past winter and early spring is indisputable evidence of the robust nature of broadband communications networks.

Nevertheless, the federal government and the communications sector are working closely together to develop best practices to promote even greater resiliency in the 2010 Communications SSP given the continual challenges and risks to network performance under crisis situations, whether natural or man-made.

A. The Cable Broadband Network Possesses Fundamental Architectural Elements and Infrastructure Design to Promote Resiliency and Survivability

Although network design varies, cable broadband networks in any particular community typically are composed of a headend, at least one distribution hub and multiple fiber nodes connected together using a mixture of fiber and coaxial cable to provide bi-directional signal paths between the operator and the customer. This hybrid fiber-coaxial (HFC) architecture is beneficial to the operator because it improves signal performance and reliability, increases available bandwidth and is easier to maintain than architectures of the past, which relied solely

on coaxial cable.[9] The headend is the point of origination and processing for most of the signals received by cable operators from external content providers, local exchange carriers, the Internet, and other networks. The headend processes and combines signals for distribution to hubs or directly to consumers. In most cases, the headend also serves as a distribution hub for the fiber nodes closest to the headend.

Distribution hubs are typically intermediate signal processing points in the network. Depending on the size of the network, more than one layer of distribution hubs may be present. These hubs are used for a variety of functions including shared use of fibers in the headend-to-distribution hub segment of the network, which reduces the number of fibers necessary to deliver signals to fiber nodes; provision of redundant signal transport between the headend and distribution hub; intermediate signal processing which improves end-of-line signal quality; and distribution of switched-service processing and aggregation equipment to reduce instantaneous demand on headend-to-distribution hub circuit capacity. The headend-to-distribution hub segment of the network is commonly built using physically and logically diverse fiber optic "ring" architectures. The design of this portion of the network is commonly used because it avoids having a single point of failure that if cut or disrupted can disable the entire network. The fiber optic lines are designed with redundant pathways so if any single line or circuit fails, the network can automatically switch to another and maintain service.

From the distribution hub or the headend, individual fiber nodes are connected which convert the optical signal into an RF signal for the "last mile" of distribution to the consumer. A fiber node consists of (1) receivers and transmitters that amplify signals as they travel away from the headend and receive upstream signals from connected coaxial legs, and (2) drop cables that

[9] *See* Walter Ciciora *et al.*, *Modern Cable Television Technology: Video, Voice and Data Communications*, (2d ed. 2004) (providing a detailed discussion of modern cable broadband networks, including architectural elements, network reliability and availability).

serve customers directly. Redundant receivers and transmitters are usually present in each node to ensure reliability. Fiber nodes are usually connected to a distribution hub using a star architecture. However, it is not uncommon for nodes to be connected to distribution hubs using redundant fiber rings in order to increase reliability. The relatively short coaxial distribution lines from the fiber nodes to the neighborhoods are not usually redundant because the effects of a disruption to a line are localized.

Building upon an already robust architecture, cable operators have taken further initiatives to improve their networks. The introduction of time-sensitive applications via the Internet such as voice services and high quality video has further stimulated network quality improvements. Such improvements include further deployment of redundancy in network elements such as CMTS (Cable Modem Termination Systems), routers and switches as well as shifts in the methodology of network testing and development.

Physical incidents can potentially impact architectural elements in a cable system but cable architecture is designed to limit network consequences within a local geographic area. Each cable operator operates distinct networks, often in different geographic regions. Thus, even the failure of a headend is likely to only disrupt service in a local or regional area.[10]

As described above, the built-in redundancies present in cable architecture are critical to outage prevention. Redundancies in the central portions of the cable operator's network include redundant fiber rings and redundant optical receivers in nodes. All outside cable plant is also usually equipped with redundant power supplies. Headends, distribution hubs, and major fiber nodes use UPS (uninterruptible power supplies) generators during commercial power outages and are maintained by self-contained fuel supplies and/or connected to natural gas facilities.

[10] In 2007, the Sector Specific Plan created by the Communications Sector Coordinating Council (CSCC) addressed the question of localization. *See generally DHS Communications Sector–Specific Plan*.

Other redundancies often built into networks include redundant processor blades and network interface cards, triggered during failures with minimal disruption to service. In general, cable systems are designed so that the closer the event is to the network core, the more safeguards are built-in to protect the network.[11]

The resilience and survivability of cable broadband network architectural elements is further enhanced by periodic testing pursuant to the Commission's rules governing the provision of cable and voice services that utilize the same network architecture as broadband Internet service.[12] Cable operators also take numerous steps to ensure high network performance and availability, such as designing their systems to handle peak usage by using reliability methodologies that model networks under certain conditions and high points of failure. This is based on widely-accepted network engineering and management best practices developed by public-private sector advisory groups and other organizations, such as the Commission's Network Reliability and Interoperability Council ("NRIC"), which preceded CSRIC. Cable operators also employ capacity modeling techniques, which involve failing one or several network links at a time and following where the traffic goes, so when failure occurs, the highly utilized circuits are already mapped and can be engineered out of the network.[13]

Beyond modeling and testing, each cable operator also has a methodology and set of tools within its own network for determining and managing congestion levels in order to prevent overloads. Network management techniques are essential to preventing network overloads during occurrences such as the snowstorms in the northeast this past winter. The network

---

[11] *See* Remarks of Richard Woundy, Senior Vice President, Software & Applications, Comcast Corporation, FCC Critical Infrastructure & Information Collection Workshop, Apr. 13, 2010.

[12] Cable operators measure the performance of their networks on at least twice each calendar year. *See* 47 C.F.R. § 76.601(b). These "Proof of Performance" measurements are a significant factor in assuring network quality.

[13] *See* Remarks of Mark Adams, Senior Director of Quality & Reliability, Cox Communications, FCC Critical Infrastructure & Information Collection Workshop, Apr. 13, 2010.

management methodology and tools used varies by operator and is typically privileged information.[14] As recently described by one leading cable broadband engineering executive, network management covers five key areas: performance management, fault management, configuration management, accounting management, and security management.[15] As she explained, it is critical for network operators "to understand how the entire ecosystem is performing on a continuous basis and establish thresholds for behaviors that would identify any impact to the customer experience."[16]

In sum, cable broadband networks achieve resilience and survivability in many ways, including secure, hardened facilities; redundancy of primary systems and network elements; and alternative routing capabilities combined with key network management techniques. There is also the human dimension to survivability. As recognized over five years ago, the Commission's Media Security and Reliability Council ("MSRC") found that cable operators have an outstanding record of emergency planning and disaster preparedness, and organizational structures to address disruptions to service or other emergency situations.[17]

---

[14] *See* Woundy, *supra* note 11.

[15] *See* Charlotte Field, Senior Vice President, Comcast Cable, *Network Operations 101*, Broadband Library 12 (Summer 2010) (performance management entails the ability to understand how your network/systems/applications ("ecosystem") are performing with respect to predefined performance measures; fault management is the ability to detect, log and understand the impact to all elements of the ecosystem and understand the impact on the customer's experience; configuration management is about ensuring that the configurations within the operator's ecosystem are at the appropriate versions of hardware and software to ensure a proper customer experience; accounting management is ensuring the operator has an understanding of the provisioning and utilization across the entire ecosystem as part of the normal course of business and tracks anomalies that might impact customer service; and security management ensures proper controls exist to ensure the operator's ecosystem is effectively protected against inappropriate access and the business understands the nature of inappropriate access.)

[16] *Id.*

[17] *See* "Communications Infrastructure Security, Access, and Restoration Working Group Final Report," February 25, 2004; http://www.fcc.gov/MSRC/.

B. The Performance of Cable Broadband Networks During Recent Natural Disasters Attests to their Resilience and Survivability

Cable operators and other broadband network providers have shown that they can withstand peak usage of their networks over a sustained period during extreme weather conditions and other natural disaster emergencies. Last winter's record-breaking snowstorms in the Mid-Atlantic states are a prime example of the successful handling of network overload with virtually no negative impact on consumers' Internet usage.

For example, the Cox high speed Internet system in Northern Virginia, which was blanketed with record snowfall that paralyzed the area for multiple days, experienced significant traffic surges as customers actively used data networks to telecommute and communicate with others in and outside the geographic area. Its capacity in not only the metro core but in the access layer was able to absorb the surge in traffic without degrading the customer experience. Similarly, Comcast reported that its networks in Washington, Philadelphia, Boston, and other communities up and down the East Coast remained operational despite significant increases in residential traffic during the snowstorms. During a winter ice storm in a remote part of New York state, which took down fiber and high voltage power lines, Time Warner Cable automatically rerouted Internet traffic through their Virginia facilities to ensure that their residential customers and business class customers' e-mail in the affected areas remained up and fully operational.

Broadband network providers have a strong interest in ensuring that the upload and download of information by customers on their networks reaches its destination in a timely, efficient manner. Network operator preparedness for emergency situations is a fundamental aspect of Internet Service Providers (ISPs) network operations. The management of the network infrastructure requires flexibility to respond to physical threats and new sources of congestion.

There is no one-size-fits-all approach among Internet engineers and network operators regarding such techniques, but there is widespread support for best practices to ensure an optimal Internet experience for customers.

II. THE EXISTING PUBLIC-PRIVATE PARTNERSHIPS UNDER THE FCC AND DHS AIMED AT PROTECTING BROADBAND COMMUNICATIONS NETWORKS ARE THE BEST APPROACH TO ADDRESSING BROADBAND NETWORK SURVIVABILITY

As the Commission is aware, a comprehensive public-private framework for addressing the ability of broadband communications networks to resist and recover from physical and other harm to network facilities and performance during natural disasters and other emergency situations is well underway. The U.S. Department of Homeland Security ("DHS") has engaged the private sector in addressing infrastructure reliability, including broadband communications networks, through various joint public-private organizations and working groups. NCTA President & CEO, Kyle McSlarrow, is a member of the President's National Security and Telecommunications Advisory Committee ("NSTAC"), and Andy Scott, NCTA's Vice President of Engineering, is a member of NSTAC's Industry Executive Subcommittee ("IES").

Through a deliberative process, NSTAC provides industry-based analyses and recommendations to the President and the executive branch regarding policy and enhancements intended to assure telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications system. Among its key areas of focus is maintaining the communications infrastructure; enhancing cyber security; assuring communications for disaster response; and addressing infrastructure interdependencies and dependencies. Reports to the President have addressed the physical

security of core networks, Internet Protocol-based priority services, and the reliance of commercial communications on the global positioning system.[18]

The National Communications System ("NCS") under DHS is an inter-agency group that also works closely with the private sector to identify, assess, and prioritize risks to communications infrastructure and key resources and design protective programs to address these vulnerabilities. Representatives from Comcast, Time Warner Cable and Cox participate in NCS activities.

In conjunction with NSTAC and DHS's working groups and task forces, NCTA representatives participate on the Communications Sector Coordinating Council ("CSCC"), a 45-member organization representing all sectors of the communications industry, including cable, commercial and public broadcasters; information service providers; satellite communications providers; utility telecommunications providers; service integrators; equipment vendors; and wireline and wireless owners and operators; as well as their respective trade associations. The CSCC, in partnership with the Communications Government Coordinating Council ("CGCC"), coordinates initiatives to improve the physical and cyber security of sector assets; to ease the flow of information within the sector, across sectors and with designated Federal agencies; and to address issues related to response and recovery under all hazards to assure the continued operation of communications services. In 2007, the CSCC completed its Sector Specific Plan ("SSP") which identified high-level, nationally critical architecture elements and is working with the CGCC on the 2010 SSP for release later this year.

---

[18] *See* Nat'l Communications System, *NSTAC Publications*, *at* http://www.ncs.gov/nstac/nstac_publications.html (last visited June 25, 2010).

In 2008, the CSCC completed work on the National Sector Risk Assessment pursuant to the government's National Infrastructure Protection Plan under DHS.[19] This qualitative work, conducted jointly by the CSCC and CGCC, assessed the risks of physical and cyber threats to the communications infrastructure. The CSCC and CGCC are working jointly to update this risk assessment in 2010.[20] Other CSCC/CGCC activities have included the development of "Communications Pandemic Influenza Planning Guidelines" for network owners and operators, including a webinar on the topic, and solutions to access and credentialing issues for communications service providers at disaster sites and implementation of emergency wireless protocols.[21]

As noted above, the Commission is taking an active role in overseeing and participating in the CSRIC process. CSRIC is charged with developing and updating best practices to ensure the availability of communications capacity during natural disasters, terrorist attacks, or other events that result in exceptional strain on the communications infrastructure. CSRIC's mission also includes best practices to ensure and facilitate "the rapid restoration of communications

---

[19] *See DHS Communications Sector–Specific Plan* at Section 3.1.

[20] *See* Press Office, DHS, *Fact Sheet, Communications Sector Specific Agencies* 2 (indicating that "the Communications SSP was last published in May 2007 and is being revised for a 2010 release"), *available at* http://www.ncs.gov/library/fact_sheets/FS-CommSec.pdf.

[21] We note that the Commission's Hurricane Katrina Independent Panel Report and Recommendations revealed serious impediments that hampered the ability of communications service providers to respond to the devastating impact of the disaster. The inability of communications repair crews to access affected areas promptly after the storm and an overall lack of coordination between public and private sector entities also greatly impeded the speed and effectiveness of restoration work. Communications infrastructure repair crews had difficulty crossing law enforcement perimeters and multiple checkpoints to access and reconstruct plant and equipment. In response, NCTA urged the Commission to work with disaster recovery agencies to accord cable operators "emergency responder" status so that they can act quickly to restore service in post-disaster areas. We also supported the Panel's recommendation that programs should make credentials available to communications repair workers, provided infrastructure workers have completed basic National Incident Management System ("NIMS") training. And we supported the Panel's call for the Commission to encourage regional, state and local Emergency Operations Centers to facilitate the inclusion of commercial communications providers, such as cable, in the priority lists for commercial power restoration of electric and other utilities. *See* NCTA Comments, *In re Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, EB Docket No. 06-119 (Aug. 7, 2006).

services in the event of widespread or major disruptions."[22] CSRIC will provide recommendations to the Commission regarding best practices to ensure optimal security, reliability, and interoperability of communications systems, across all platforms – telecommunications, media and public safety communications systems.

Cable executives serving on CSRIC include Glenn A. Britt, Chairman, President & CEO, Time Warner Cable; Patrick Esser, President, Cox Communications; and John Schanz, Executive Vice President, National Engineering and Technology Operations, Comcast Corporation.

CSRIC has designated eight working groups and subgroups to address the full range of public safety and broadband network survivability and related issues. Senior technical, network operations, and security executives from the cable industry are serving on several key working groups. Working Group 6, for example, is addressing best practices to enhance security, reliability, operability and resiliency of communications infrastructure, taking into account previous recommendations of NRIC and MSRC. Working Group 2B is devoted entirely to reviewing and updating MSRC best practices, last reviewed in 2005. Working Group 7 is addressing overload issues for communications networks caused by the outbreak of a pandemic, with emphasis on priority service requirements – this group is specifically tasked with developing a strategy to assess the order of magnitude of users potentially affected, the types of services affected, the process for authorizing prioritized communications, performance standards and metrics, and expected costs.[23]

---

[22] Charter of the FCC's Communications Security, Reliability, and Interoperability Council 1, *available at* http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf.

[23] *See CSRIC Working Group Descriptions*, *available at* http://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf. Other working groups include Working Group 8, ISP Network Protection Practices, which will investigate current practices that ISPs use to protect their networks from harms caused by the logical connection of computer equipment, as well as desired practices and associated implementation obstacles, and Working Group 2A, Cyber Security Best Practices, which will review cyber security best practices based on previous work under NRIC VI and VII.

In light of the diverse array of threats to Internet communications, the Commission also should consider expanding the membership of CSRIC and establishing additional working groups to ensure that the entire physical infrastructure of the Internet, and not just ISP networks, remain reliable and secure.

In addition to the federal initiatives in this area, cable industry engineers in network operations and management widely participate in a host of cable-specific working groups and activities of the Society of Cable Telecommunications Engineers ("SCTE"). SCTE is a non-profit professional association that creates technical standards, protocols, and best practices used by the cable industry. As part of its services, SCTE provides an American National Standards Institute-accredited forum for the development of technical specifications supporting the cable industry which is recognized by the International Telecommunications Union ("ITU"). As the leading resource for standards and best practices for cable companies, SCTE's guidelines and protocols produced by its working groups are routinely utilized by cable operators.[24]

Recently, SCTE created a new operations forum designed to enhance current standards, information, and best practices for cable network infrastructure and management. The forum's target areas are:

- efficient facilities management;
- intelligent network operations tools including signature analysis, failure modes, redundancy, and backup powering;
- disaster recovery best practices, including network recovery in hazardous conditions;
- security best practices, including physical headend security;
- wireless/wi-fi integration; and
- energy management.

[24] *See generally* SCTE, *About Us*, *at* http://www.scte.org/content/index.cfm?pID=157 (last visited June 11, 2010).

In sum, cable broadband network providers are committed to the public-private partnership model and to the internal assessment and reassessment of the strength and flexibility of their networks under adverse conditions. The emphasis on public-private initiatives has resulted in mutually beneficial information-sharing mechanisms and the implementation of programs to maintain a reliable and resilient communications infrastructure.

It is important to note, however, that the collaboration among the various government and private sector partners is premised on a system of voluntary information-sharing between the private sector and DHS.[25] Moreover, as GAO reported in 2009, DHS found that "requiring private entities to provide sensitive information to the department conflicts with the voluntary information-sharing approach DHS was to pursue under the Homeland Security Act."[26] Similarly, the Commission's CSRIC presumably operates under the same confidentiality and voluntary information-sharing procedures.

Yet the NOI seeks to elicit highly sensitive and confidential information from network providers *for the public record*, such as vulnerabilities in the broadband infrastructure and the methodologies that network operators employ to handle sudden surges in broadband use, as well as the limits of such techniques. From a public safety and national security perspective, we caution the Commission not to gather such information in a public proceeding, but rather rely on the existing federal public-private information-sharing framework. A public proceeding will only provide fodder for those who wish to exploit or otherwise harm the nation's broadband communications infrastructure.

---

[25] *See GAO Critical Infrastructure Report* at 3.

[26] *Id*. at 3, n.7 (citing General Accountability Office, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, GAO-09-654R (June 2009)).

III. THE COMMISSION SHOULD ENCOURAGE A BROAD APPROACH THAT ENCOMPASSES THE VARIED THREATS TO BROADBAND INTERNET COMMUNICATIONS

The cable industry supports continued reliance on broad-based, public-private partnerships that build upon the collaborative, consensus-based approach that has helped ensure the reliability and resiliency of the Internet thus far. Importantly, threats to the reliability and resiliency of the Internet today are not located solely on the underlying networks, but can be found throughout the entirety of the Internet's ecosystem.[27] It would not serve the public interest if broadband Internet access facilities remained up and running but key communications were hampered by attacks affecting some other vulnerability in the Internet ecosystem.

[27] *See e.g.* Google Inc., Form 10-K, for fiscal year ended Dec. 31, 2009 at 22, 26; AOL Inc., Form 10-K, for fiscal year ended Dec. 31, 2009 at 21.

CONCLUSION

The cable industry believes that market forces, paired with government collaboration and support, have and will continue to drive reliable and resilient broadband communications networks. As noted by the National Infrastructure Advisory Council:

> The challenge facing government is to maintain its role in protecting critical infrastructures, while determining how best to encourage market forces to improve the resilience of companies, provide appropriate incentives and tools to help entire sectors become resilient, and step in when market forces alone cannot produce the level of infrastructure security needed to protect citizens, communities, and essential economic systems.[28]

In promoting the survivability of broadband network communications, the Commission should also bear in mind the complexity of the broadband ecosystem and the need for the development of comprehensive solutions through the public-private framework. The Commission should rely on CSRIC as the centerpiece of its efforts in this area and it should promote flexibility and innovation in combating ongoing threats to network infrastructure in addressing future public safety and homeland security objectives.

Respectfully submitted,

/s/ Neal M. Goldberg

Neal M. Goldberg
Loretta P. Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

Andy Scott
Vice President, Engineering

Stephanie B. Power
Research Assistant

June 25, 2010

[28] *GAO Critical Infrastructure Report* at 4 (quoting Nat'l Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations* (Sept. 8, 2009)).