



**National Cable & Telecommunications Association**  
25 Massachusetts Avenue, NW – Suite 100  
Washington, DC 20001  
(202) 222-2300  
  
www.ncta.com

**Loretta Polk**  
Vice President and Associate General Counsel  
  
(202) 222-2445  
(202) 222-2446 Fax

September 23, 2010

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, D.C. 20554

**Re: PS Docket No. 10-146; GN Docket No. 09-51**

Dear Ms. Dortch:

On August 9, 2010, the Commission issued a *Public Notice* seeking comment on the *National Broadband Plan* recommendation to create a Cybersecurity Roadmap.<sup>1</sup> The Notice asks for public input on “the most vital cybersecurity vulnerabilities for communications networks or users” in conjunction with establishing a two-year plan on how those vulnerabilities can be addressed.<sup>2</sup> The cable industry supports the ongoing public-private sector collaborative efforts to identify cyber threats and vulnerabilities in the broadband Internet ecosystem and the development of countermeasures and solutions to respond to such global threats.

In that regard, the National Cable & Telecommunications Association (“NCTA”) hereby submits for the record its comments filed in GN Docket Nos. 09-47, 09-51, 09-137 (*In re Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*); PS Docket No. 10-92 (*In re Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*); and PS Docket No. 10-93 (*In re Cyber Security Certification Program*). NCTA respectfully requests that the Commission incorporate the enclosed comments into the record in the instant proceeding.

As reflected in the attached filings, the cable industry is committed to the Commission’s overarching goal to enhance the security of the nation’s broadband communications infrastructure from existing and emerging cyber attacks. However, as NCTA cautioned in recent comments, “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

---

<sup>1</sup> Public Notice, FCC, *FCC Seeks Public Comment on National Broadband Plan Recommendations to Create a Cybersecurity Roadmap*, DA 10-1354 (Aug. 9, 2010) (“*Public Notice*”).

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

those who wish to harm the nation's broadband communications infrastructure.”<sup>3</sup> Rather than identifying “the five most critical cybersecurity threats to the communications infrastructure and its end users”<sup>4</sup> in a public proceeding, we again urge the Commission to rely on its Communications, Security, Reliability, and Interoperability Council (“CSRIC”), as well as other public-private sector cybersecurity initiatives at the U.S. Department of Homeland Security, to drive efforts to address cyber security threats.<sup>5</sup> In particular, CSRIC’s Working Group 2A is charged with developing cyber security best practices. Cable industry representatives are active members on this and other CSRIC working groups.

Public-private sector initiatives allow flexibility and promote innovation in combating cyber security threats. Indeed, the Government Accountability Office recently reported that the communications sector received the highest marks among the five critical infrastructure sectors in meeting public sector stakeholders’ expectations in ten categories of expected services, including commitment to execute plans and recommendations, such as best practices.<sup>6</sup> We believe that these forums are working and are best suited to provide recommendations to the federal government on steps to ensure optimal security and reliability of communications systems in the face of evolving cyber threats.

If any questions arise concerning this matter, please contact the undersigned.

Respectfully submitted,

**/s/ Loretta Polk**

Andy Scott  
Vice President, Engineering  
Science & Technology

Loretta Polk  
Stephanie L. Poday  
Counsel for the National Cable &  
Telecommunications Association

Enclosures

---

<sup>3</sup> NCTA Comments, *In re Effects on Broadband Communications Networks Of Damage to or Failure of Network Equipment or Severe Overload*, PS Docket No. 10-92, at 4 (June 25, 2010).

<sup>4</sup> *Public Notice* at 1.

<sup>5</sup> See NCTA Cyber Security Certification Program Comments at 6. *See id.* at 2, 8; NCTA Comments, *NBP Public Notice #8*, GN Docket Nos. 09-47, 09-51, and 09-137, at 6-7 (Nov. 12, 2009); NCTA Survivability Comments, PS Docket No. 10-92, at 12-16.

<sup>6</sup> U.S. Gov’t Accountability Office, *Critical Infrastructure Protection, Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628, at 21, table 6 (July 2010).



aspects of broadband services.<sup>1</sup> The Commission notes that broadband offers a variety of potential benefits to emergency responders and other public safety agencies and that, among other things, improved broadband services could enhance public safety’s ability to provide warnings and other information to Americans in times of emergency. The Commission points out, however, that “achieving these potential public safety benefits also requires consideration of how to implement and maintain a broadband infrastructure that is resilient in the face of cyber attacks and similar threats to network security.”<sup>2</sup>

As the White House’s Cyberspace Policy Review, released in May 2009, makes clear “the globally-interconnected digital information and communications infrastructure known as “cyberspace” underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security.”<sup>3</sup> Broadband services are a vital component of the economic and social fabric of American society. As recognized by various parties in this proceeding, “without an effective and comprehensive cybersecurity strategy, all broadband-enabled services, including e-commerce, telemedicine, smart grids, telecommunity, inventory tracking, voice and video conferencing, and others, would be vulnerable to serious disruption.”<sup>4</sup>

Today’s communications infrastructure processes and transmits vast amounts of information at faster and faster speeds over highly complex and integrated networks. A variety of bad actors are exploiting vulnerabilities at all levels of this infrastructure – in the networks,

---

<sup>1</sup> NBP Public Notice #8, GN Docket Nos. 09-47, 09-51, 09-137, rel. Sept. 28, 2009.

<sup>2</sup> *Id.* at 1.

<sup>3</sup> *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009, [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

<sup>4</sup> *In the Matter of A National Broadband Plan for Our Future*, GN Docket No. 09-51, Comments of AT&T Inc June 8, 2009 at x; *see also* Comments of Verizon and Verizon Wireless and United States Telecom Association, GN Docket No. 09-51, June 8, 2009.

operating systems, applications and end-user points – and as the Commission recently recognized, such attacks are increasingly more sophisticated yet easier to execute.<sup>5</sup> The challenge is even more daunting as cyber attacks are often difficult to trace because the perpetrators are located across the globe. Network providers widely agree that the ability to deploy innovative tools to combat cyber threats, as part of comprehensive, coordinated public-private sector efforts, is a critical part of securing and safeguarding the nation’s broadband future, and should be incorporated into the Commission’s national broadband plan.

NCTA is pleased to provide additional comments on the cable industry’s efforts to address cybersecurity, its involvement in various public-private sector initiatives, and the importance of government policies that allow flexibility and innovation in combating the problem.

**I. CABLE OPERATORS HAVE IMPLEMENTED EXTENSIVE NETWORK-BASED AND CUSTOMER-BASED CYBERSECURITY MEASURES AND CAPABILITIES**

---

As the nation’s largest provider of high-speed Internet service, the cable industry and its customers are experiencing the full range of “cyber threats,” including viruses, worms, spam, malware, spyware and denial-of-service attacks. Comcast discussed a problem that is replicated in cable broadband services throughout the industry in its comments in the national broadband plan proceeding:

Each month, Comcast handles millions of customer reports about spam and phishing, and blocks an estimated 11.5 billion spam, virus, and phishing messages – online activities that consume large amounts of bandwidth and pose serious threats to customer privacy and security, not to mention the impact to the user experience.<sup>6</sup>

---

<sup>5</sup> September Commission Meeting, Broadband Task Force presentation, Sept. 29, 2009, slide 166 depicting increasing variety and sophistication of attack modes.

<sup>6</sup> *In the Matter of A National Broadband Plan for Our Future*, GN Docket No. 09-51, Comcast Comments at 26-27.

Cable operators, along with other private sector network operators, are engaged in a host of measures to maintain the integrity of the networks and protect their customers against such harm. Cable operators have invested substantial resources to deploy state-of-the-art technologies and applications in their networks to combat all forms of malicious and harmful Internet activities.

At the customer level, cable operators have instituted comprehensive cyber and related online security programs to manage the Internet safety and security of their customers. These programs provide free tools and software to enable cable customers to protect their computers from cyber-attacks and loss or corruption of data.

For example, Comcast recently enhanced its online security program with a new service called “Constant Guard,” which is designed to protect its high-speed Internet customers from bots, viruses and other online threats.<sup>7</sup> The program is the culmination of a multi-year effort to assemble a dedicated team of security professionals, implement best-in-class security software and establish a Security Web portal of consumer resources to protect customers from increasingly sophisticated online threats. Constant Guard provides customers, at no charge, the McAfee Internet Security Suite and the Comcast Toolbar, which contains a variety of security tools, including spyware detection and removal, anti-phishing and anti-virus software. The program also provides an online Security Channel, which includes real-time security alerts, tips, tools and other resources that help educate and protect consumers.

In October 2009, Comcast also announced that it is conducting a trial of an in-browser “Service Notice” that will alert customers who appear to have one or more home computers

---

<sup>7</sup> “Comcast Unveils Comprehensive “Constant Guard” Internet Security Program, Announces Dedicated Customer Security Assurance Team, Launches Proactive Service Notice for High-Speed Internet Customers Whose PCs May Be Infected by Bots,” Press Release, October 8, 2009; “Comcast Maintains Anti-Bot Initiative,” Communications Technology, Nov. 10, 2009; *see also* <http://www.comcast.com/customers/faq/FaqDetails.aspx?ID=2620&fss=security>.

infected with a bot or virus. The notification will consist of a message that will appear while a customer is surfing the Web.<sup>8</sup> The message will notify the customer that there may be a bot on their computer and gives them the option to use the company's Anti-Virus Center for information on how to clean the computer. According to the National Cyber Security Alliance, bots (or botnets) are the Internet's fastest-growing cyber crime and, based on their survey data, 71% of consumers are unaware of this online threat.<sup>9</sup> With servers typically outside the U.S., bots are the leading cause of spam and are frequently the culprits in identity theft, information theft and denial-of-service attacks.

Time Warner Cable provides a comprehensive suite of security programs and solutions free to its Road Runner Internet service customers. In particular, Road Runner offers the CA Internet Security Suite, a personal Internet security service that provides comprehensive protection against viruses, hackers, identity theft, spyware, spam, offensive websites and other online threats "that can jeopardize your privacy, your data, and your PC's performance."<sup>10</sup> CA Security Suite includes anti-virus, anti-spyware and anti-spam software, as well as a personal firewall to block malicious programs and prevent PC intruders. Cox offers an easy-to-use Security Center and Security Suite that gives its customers one-click access to security information to enable them to control and protect their computers. Customers can easily scan their computer, check for updates and configure their security settings.<sup>11</sup>

---

<sup>8</sup> *Id.*

<sup>9</sup> National Cyber Security Alliance Press Release, "Seventy-One Percent of Consumers Lack Knowledge on the Internet's Fastest Growing Cyber Crime Threat, Botnets," at (<http://staysafeonline.mediaroom.com/index.php?s=43&item=11>); see e.g. "Security Firm Chokes Sprawling Spam Botnet", The Register, November 10, 2009 at [http://www.theregister.co.uk/2009/11/10/fireeye\\_takes\\_out\\_ozdok/](http://www.theregister.co.uk/2009/11/10/fireeye_takes_out_ozdok/).

<sup>10</sup> [http://help.rr.com/HMSLogic/security\\_abuse\\_help\\_topic.aspx](http://help.rr.com/HMSLogic/security_abuse_help_topic.aspx); see also Time Warner Cable Comments in national broadband plan proceeding, GN Docket 09-51, June 8, 2009 at 13.

<sup>11</sup> See e.g. Cox security suite powered by McAfee with antispyware, anti-spam, anti- identity theft features: [http://ww2.cox.com/residential/northernvirginia/internet/cox-security-suite.cox?campcode=goog\\_internet](http://ww2.cox.com/residential/northernvirginia/internet/cox-security-suite.cox?campcode=goog_internet).

Similarly, Charter, Cablevision, Bright House, Insight and other cable operators provide comprehensive security services to their broadband customers in conjunction with CA or other state-of-the-art security applications.<sup>12</sup> Many cable operators also provide updates on the latest threats, ways for customers to report security violations on their systems, such as spam, hackers and other threats, and advice on how to remove offending malware.

## **II. THE CABLE INDUSTRY IS COMMITTED TO THE PUBLIC-PRIVATE PARTNERSHIP MODEL AND THE DEVELOPMENT OF BEST PRACTICES**

As the Commission is aware, the federal government, notably the U.S. Department of Homeland Security (DHS), is addressing cybersecurity through various joint public-private study and planning efforts and organizations. Recent cybersecurity policy work around existing and emerging threats has been undertaken through the executive branch's National Cybersecurity Initiative and the White House 60-Day Cyberspace Policy Review, among other initiatives, as well as ongoing legislative activity.<sup>13</sup>

The cable industry participates in various public-private sector initiatives that contribute to the foregoing policy work and the broader public safety and homeland security policy challenges. NCTA President & CEO, Kyle McSlarrow, is a member of the President's National Security and Telecommunications Advisory Committee ("NSTAC"). NSTAC provides industry-based analyses and recommendations to the President and the executive branch regarding policy and enhancements to national security and emergency preparedness of the nation's

---

<sup>12</sup> See e.g. [http://help.rr.com/HMSFaq/e\\_CAISS.aspx](http://help.rr.com/HMSFaq/e_CAISS.aspx); <http://www.bhnc.com/>; <http://www.charter.com/Customers/supportgeneral.aspx?pagetype=1>; <http://www.optimum.net/Lifestyle/MyComputer/Security>; <http://optimum.custhelp.com/>.

<sup>13</sup> See e.g. "Cybersecurity: Current Legislation, Executive Branch Initiatives, Options for Congress," Congressional Research Service, Sept. 30, 2009 at <http://www.fas.org/sgp/crs/natsec/R40836.pdf>. On May 29, 2009, President Obama issued the 60-day review findings and near-term action plan, which are aimed at "developing a strategic framework to ensure that the U.S. government's initiatives are appropriately integrated, resourced, and coordinated," notably announcing the appointment of a cybersecurity official to coordinate interagency strategy and policy.

communications systems. Among its key areas of focus is enhancing cyber security and maintaining the global communications infrastructure.

Earlier this year, NSTAC recommended the establishment of a joint, integrated public-private, round-the-clock cyber-incident detection, prevention, mitigation, and response capability to address cyber-attacks of national consequence.<sup>14</sup> In particular, to combat botnets, it recommended increased international cooperation and partnerships and the development of international cyber-incident warning and response capabilities.

In conjunction with NSTAC and DHS's policy working groups and task forces, NCTA representatives participate on the Communications Sector Coordinating Council (CSCC), a 40-member organization representing all sectors of the communications industry, including cable, broadcasting, Internet service providers, wireline and wireless service providers, satellite, undersea cable, public utilities and others. CSCC coordinates, among other things, industry-led initiatives to improve the physical and cyber security of communications sector assets. In 2008, the CSCC completed work on the National Sector Risk Assessment pursuant to the government's National Infrastructure Protection Plan under DHS.<sup>15</sup> This qualitative work, conducted jointly by the CSCC and the Communications Government Coordinating Council (CGCC), assessed the risks of physical and cyber threats to the communications infrastructure. CSCC is currently working on a communications sector plan, which will address specific cybersecurity policies and practices.

Cable executives also are serving on the Commission's recently-chartered federal advisory committee, the Communications Security, Reliability, and Interoperability Council

---

<sup>14</sup> NSTAC, "Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability", May 21, 2009.

<sup>15</sup> See e.g. U.S. Department of Homeland Security, "Communications, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan", May 2007.

(CSRIC), including 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 will provide recommendations to the Commission regarding best practices and action the Commission can take to ensure optimal security, reliability, and interoperability of communications systems, across all platforms – telecommunications, media and public safety communications systems. CSRIC’s charter calls for the Council to develop new best practices to “[t]ake into account new and advanced technologies including broadband and IP-based technologies.”<sup>16</sup>

A common thread that has emerged from the ongoing, multi-faceted cybersecurity policy initiatives is the need for greater coordination and collaboration between government and network service providers to further cybersecurity objectives. The cable industry is committed to working with all stakeholders in a coordinated, collaborative manner to pursue solutions to reduce significantly the vulnerability of the nation’s broadband networks to cyber threats.<sup>17</sup>

For their part, all broadband service providers need the ability to innovate and deploy intelligence in the network to combat cyber crime. Meeting the technical challenges of securing broadband infrastructure requires constant network upgrading and responsiveness to new and emerging threats. As the Obama Administration’s Cyberspace Policy Review notes, “the

---

<sup>16</sup> CSRIC Charter at 1. Comcast and other companies are also addressing network security and related matters through such private sector organizations as Messaging Anti-Abuse Working Group, the Anti-Phishing Working Group, the North American Network Operators Group and the Internet Engineering Task Force.

<sup>17</sup> *See also* Verizon and Verizon Wireless Comments, GN Docket No. 09-51, June 8, 2009 at 6 (“increased level of coordination and cooperation among public and private stakeholders will be essential in order to tackle the complex and daunting challenge of cybersecurity. At the same time, encouraging continued innovation in broadband networks and services – such as by encouraging the deployment of technology that makes networks smarter and more capable of fending off and responding to attacks – will be required.”).

Federal government . . . must be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security.”<sup>18</sup>

Moreover, ensuring that network providers have the flexibility and tools needed to address network security is also fundamental to broadband adoption strategies.<sup>19</sup> Reluctant broadband adopters need confidence in the networks in order to overcome fears and other concerns that prevent them from utilizing broadband services. As Verizon succinctly explained:

In order to effectively address the evolving and significant threats that exist online – and to foster the level of comfort and security needed to encourage consumers to go online – policymakers should encourage providers to develop and employ a variety of innovative tools and approaches that improve cybersecurity.<sup>20</sup>

We are encouraged by the Commission’s proposals in the recently adopted Notice of Proposed Rulemaking on net neutrality that “broadband Internet access service providers may address harmful traffic or traffic unwanted by users as a reasonable network management practice.”<sup>21</sup> In proposing that broadband providers may take other reasonable steps to maintain the proper functioning of their networks, the Commission further states that “we do not presume to know now everything [broadband Internet access service providers] may need to do to provide robust, safe, and secure Internet access to their subscribers, much less everything they may need

---

<sup>18</sup> White House Cyberspace Policy Review Report at 31.

<sup>19</sup> See e.g. “Barriers to Broadband Adoption: A Report to the Federal Communications Commission”, The Advanced Communications Law & Policy Institute, New York Law School, October 2009 (reflecting security issues as one of the barriers to adoption); see also Time Warner Cable Comments and Cox Communications Comments, GN Docket No. 09-51, June 8, 2009.

<sup>20</sup> See e.g. Verizon Comments at 6 (noting President Obama’s statement that cybersecurity “is one of the most serious economic and national security challenges we face as a nation”, requiring government to “collaborate with industry to find technology solutions that ensure our security and promote prosperity” and to “continue to invest in cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time.”).

<sup>21</sup> In *the Matter of Preserving the Open Internet, Broadband Industry Practices*, Notice of Proposed Rulemaking, GN Docket No. 09-191, WC Docket No. 07-52, rel. October 22, 2009 at ¶ 138.

to do as technologies and usage patterns change in the future.”<sup>22</sup> And it is helpful that the Commission recognizes that “additional flexibility to engage in network management provides network operators with an important tool to experiment and innovate as user needs change.”<sup>23</sup>

### **CONCLUSION**

As outlined above, the Commission should incorporate into the national broadband plan ongoing public-private initiatives aimed at securing the nation’s digital infrastructure from growing cyber threats. And it should promote policies that foster the development and deployment of innovative applications and tools to improve cybersecurity and address burgeoning threats to consumers.

Respectfully submitted,

**/s/ Neal M. Goldberg**

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

November 12, 2009

---

<sup>22</sup> *Id.* at ¶ 140.

<sup>23</sup> *Id.*

**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

June 25, 2010

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

**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.<sup>1</sup>

**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.”<sup>2</sup>

---

<sup>1</sup> 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.

<sup>2</sup> *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 21<sup>st</sup> 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.”<sup>3</sup> 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

---

<sup>3</sup> 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.<sup>4</sup>

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

---

<sup>4</sup> 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.”<sup>5</sup> 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.

---

<sup>5</sup> 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.”*<sup>6</sup> 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.<sup>7</sup>

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.”<sup>8</sup> 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

---

<sup>6</sup> 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>.

<sup>7</sup> GAO *Critical Infrastructure Report* at 25.

<sup>8</sup> *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.<sup>9</sup> 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

---

<sup>9</sup> 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.<sup>10</sup>

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.

---

<sup>10</sup> 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.<sup>11</sup>

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.<sup>12</sup> 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.<sup>13</sup>

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

---

<sup>11</sup> See Remarks of Richard Woundy, Senior Vice President, Software & Applications, Comcast Corporation, FCC Critical Infrastructure & Information Collection Workshop, Apr. 13, 2010.

<sup>12</sup> 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.

<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup> 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.”<sup>16</sup>

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.<sup>17</sup>

---

<sup>14</sup> See Woundy, *supra* note 11.

<sup>15</sup> 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.)

<sup>16</sup> *Id.*

<sup>17</sup> 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.<sup>18</sup>

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.

---

<sup>18</sup> See Nat’l Communications System, *NSTAC Publications*, at [http://www.ncs.gov/nstac/nstac\\_publications.html](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.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup>

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

---

<sup>19</sup> See *DHS Communications Sector-Specific Plan* at Section 3.1.

<sup>20</sup> 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](http://www.ncs.gov/library/fact_sheets/FS-CommSec.pdf).

<sup>21</sup> 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.”<sup>22</sup> 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.<sup>23</sup>

---

<sup>22</sup> 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](http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf).

<sup>23</sup> 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.<sup>24</sup>

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.

---

<sup>24</sup> 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.<sup>25</sup> 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.”<sup>26</sup> 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.

---

<sup>25</sup> See GAO Critical Infrastructure Report at 3.

<sup>26</sup> *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.<sup>27</sup> 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.

---

<sup>27</sup> 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.<sup>28</sup>

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**

Andy Scott  
Vice President, Engineering

Stephanie B. Power  
Research Assistant

June 25, 2010

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

---

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

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

In the Matter of )  
 )  
Cyber Security Certification Program ) PS Docket No. 10-93

**COMMENTS OF  
THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association (“NCTA”) hereby submits its comments in response to the Notice of Inquiry (“*Notice*”) issued by the Commission in the above-captioned proceedings.<sup>1</sup> In the *Notice*, the Commission seeks comment on “whether [it] should establish a voluntary program under which participating communications service providers would be certified by the FCC or a yet to be determined third party entity for their adherence to a set of cyber security objectives and/or practices.”<sup>2</sup> Such a program is unnecessary and would not advance the Commission’s objectives in this area.

**INTRODUCTION AND SUMMARY**

The cable industry supports the Commission’s overarching goal to enhance the security of the nation’s broadband communications infrastructure from existing and emerging cyber attacks. Today’s globally-interconnected, highly complex digital information and communications infrastructure, or “cyberspace,” is experiencing serious threats at all levels – in the networks, operating systems, applications, and end-user points – and such threats are

---

<sup>1</sup> 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.

<sup>2</sup> *In re Cyber Security Certification Program*, Notice of Inquiry, 25 FCC Rcd 4345 ¶ 1 (2010) (“*Notice*”).

increasingly more sophisticated, harder to trace, and easier to execute from outside of U.S. borders. Combating these complexities requires comprehensive and nimble solutions that recognize and integrate the inter-related and inter-dependent entities and functions that comprise the Internet ecosystem.

As with the Commission's companion effort to promote the survivability and reliability of the broadband network infrastructure, cyber security is actively being addressed in multiple public-private sector initiatives. The FCC's Communications, Security, Reliability, and Interoperability Council ("CSRIC"), for instance, is an important forum for developing best practices and voluntary mechanisms to meet the Commission's cyber security objectives, while promoting the use of innovative and flexible tools to respond to real-time cyber incidents and threats. And the U.S. Department of Homeland Security has engaged the private sector in a number of joint public-private initiatives to comprehensively assess and address these threats. While well-intentioned, a cyber security certification program as contemplated in the *Notice* could undermine these ongoing efforts to safeguard the nation's broadband communications infrastructure. Indeed, regulation of Internet network providers and others in the Internet ecosystem that are equally subject to cyber attacks, even through a voluntary certification program, could inhibit efforts to better secure the Internet from a host of ever-changing threats.

The cable industry believes that the Commission should rely on the ongoing best practices and voluntary standardization efforts, rather than impose a new government-sponsored cyber security certification program. The commitment of broadband network providers to best practices and other safeguards is evident from the participation of senior executives in CSRIC and its working group devoted entirely to cyber security.

There is no need for a certification program to “create business incentives for providers of communications services to sustain a high level of cyber security culture and practice”<sup>3</sup> and promote “market incentives”<sup>4</sup> for broadband communications providers to upgrade the cyber security measures that apply to their networks. In a highly competitive broadband environment, broadband network providers have every incentive to provide dependable and secure broadband communications to their customers. It is squarely within their economic interest to do so.

**I. THE CREATION OF A GOVERNMENT-SPONSORED CERTIFICATION PROGRAM WOULD NOT ADVANCE THE FEDERAL GOVERNMENT’S CYBER SECURITY OBJECTIVES AND WOULD BE COUNTERPRODUCTIVE TO THE EXISTING PUBLIC-PRIVATE SECTOR CYBER SECURITY FRAMEWORK**

---

The Commission’s concerns regarding cyber security are wholly warranted and fully shared by the cable industry. The value that cable operators offer their customers in providing Internet service would be seriously undermined if consumers’ Internet transactions, their personal information, and the availability of a secure Internet were cast into doubt. Cable operators also share with other providers of services across the Internet ecosystem a responsibility to protect and prevent breaches of this network of networks upon which the entire nation’s economy and security increasingly depends.

To the extent that we have concerns about the Commission’s proposals in this proceeding, they are concerns over means, not ends. The constantly evolving nature of the Internet’s infrastructure and technology, as well as the content and applications available on the Internet, requires a swiftness and flexibility in developing approaches to cyber security and responding to

---

<sup>3</sup> Notice ¶ 1.

<sup>4</sup> *Id.* ¶ 9.

new threats. Moreover, cyber security measures, to be effective, must themselves be developed and implemented in a secure environment that minimizes the opportunity of those who seek to breach Internet security to anticipate and defeat such measures.

A centralized cyber security initiative that is coordinated and supervised by the Commission is not the optimal environment in which to ensure either of these necessary components. The Commission appears to contemplate a set of procedures to establish “general network cyber security objectives” and a “list of network cyber security criteria.”<sup>5</sup> And once such procedures and criteria are established, it anticipates a process for reviewing and revising such criteria, as well as a certification program under which it, or various private entities, should

(1) be responsible for developing, maintaining and improving the list of network cyber security criteria; (2) have responsibility for accrediting the auditors who will conduct security assessments of communications service providers; (3) establish the assessment procedures and practices to guide those assessments; and (4) maintain a database of the communications services providers that have passed the assessments and are therefore entitled to market their services as meeting the FCC’s cyber security certification requirements.<sup>6</sup>

The Commission suggests that it have responsibility for establishing and reviewing the standards and criteria, that private sector entities be responsible for “the daily operation” of the program, and that the Commission “serve as a final route of appeal” of certification determinations.<sup>7</sup>

This regime of standard setting, certification and appeals is far too rigid and cumbersome for the problem at hand. As the Obama Administration’s *Cyberspace Policy Review* notes, the Federal government should “be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security.”<sup>8</sup> What is needed are cooperative public-

---

<sup>5</sup> *Id.* ¶¶ 18, 23.

<sup>6</sup> *Id.* ¶ 23.

<sup>7</sup> *Id.* ¶ 24.

<sup>8</sup> *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure* 31, May 2009, available at [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

private efforts to deal with unanticipated problems when they arise, not general standards and criteria that are based on threats that have arisen in the past.<sup>9</sup> The standard setting, auditing, certification, and appeals processes will simply impede responsiveness to threats, as well as add costs to and divert resources from the urgent efforts of Internet stakeholders to combat cyber security threats and incidents on an ongoing basis.

Moreover, centralizing efforts to ensure cyber security in a single standard setting and certification program is likely to be less effective than encouraging the development of cyber security measures in various forums and organizations. A Commission-supervised approach to establishing and certifying compliance with a certification program may have the result of stifling innovation and experimentation with alternative approaches – precisely the opposite of what is needed to ensure maximum ongoing protection. The incentive to maintain a Commission “seal of approval” may, in other words, impede efforts to develop innovative approaches to dealing with ever-changing threats.

Centralizing deliberations and standardized approaches regarding cyber security problems under the auspices of the Commission would not only impair effectiveness in dealing with security risks, it could also facilitate security breaches. A common set of Government sanctioned standards and protocols – along with a public identification of entities that are (or, by

---

<sup>9</sup> We note that various third party entities regularly monitor the performance and vulnerabilities of broadband communications, which are confronted with increasingly sophisticated cyber attacks, including botnets, malware, and spyware. *See, e.g.*, Arbor Networks, *ATLAS, About* (“Arbor collectively analyzes the data traversing disparate “darknets” to develop a truly globally scoped view into malicious traffic traversing the backbone networks that form the Internet’s core. With this vantage point, Arbor is uniquely positioned to deliver enterprise and service provider-specific intelligence about malware, exploits, phishing and botnets beyond that being delivered by any other entity today. ATLAS delivers an unprecedented view into Internet scale activity and the ability to discern what new attacks are on the horizon.”), at <http://atlas.arbor.net/about/> (last visited July 7, 2010). Consumer-oriented products and services are also available to combat cyber threats. *See, e.g.*, NCTA Comments, *NBP Public Notice #8*, GN Docket Nos. 09-47, 09-51, and 09-137, at 4 (Nov. 12, 2009) (“*NCTA Cyber Security Comments*”) (describing Comcast’s Constant Guard solution, which is designed to protect its high-speed Internet customers from bots, viruses, and other online threats, and is offered to Comcast’s broadband customers at no charge).

implication, are not) – certified as in compliance with those standards and protocols would make it easier for cyber criminals to circumvent security measures and locate the “soft spots” in the ecosystem’s security. Transparency is generally a virtue in public standard setting, but it can be counterproductive when those standards are intended to defeat cyber crime.

This is not to say that collaborative efforts among stakeholders across the Internet ecosystem are not beneficial. To the contrary, they may be essential. But, as discussed below, forums already exist for facilitating such efforts – forums that are more conducive to ensuring the flexibility, the diversity of approaches, and the security that are necessary to the effective protection of the Internet and its users.

## **II. CSRIC PROVIDES A VALUABLE FORUM FOR ADDRESSING THREATS TO CYBER SECURITY, AND SHOULD DRIVE THE COMMISSION’S EFFORTS IN THIS AREA**

The Commission’s forum for coordinating cyber security efforts among a cross-section of communications providers is CSRIC. CSRIC’s mission is “to provide recommendations to the FCC to ensure optimal security, reliability, and interoperability of communications systems, including public safety, telecommunications, and media communications.”<sup>10</sup> Recommendations from CSRIC will also address “ensuring the availability of communications capacity during natural disasters, terrorist attacks, or other events that result in exceptional strain on the communications infrastructure” and “ensuring and facilitating the rapid restoration of communications services in the event of widespread or major disruptions.”<sup>11</sup> Efforts are already underway through the CSRIC working groups to develop approaches to complicated cyber security issues. For example, Working Group 2A is devoted to taking “a fresh look at cyber

---

<sup>10</sup> FCC, *Charter of the FCC’s Communications Security, Reliability, and Interoperability Council* ¶ 3, available at [http://www.fcc.gov/pshs/docs/advisory/csric/CSRC\\_charter\\_03-19-2009.pdf](http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf).

<sup>11</sup> *Id.*

security best practices, including [best practices covering] all segments of the communications industry and public safety communities.”<sup>12</sup>

The Commission should make the work of CSRIC a top priority.<sup>13</sup> As the Chairman explained at the first CSRIC meeting:

We are fortunate to have in this room a combination of talent and experience from different professional disciplines and from all segments of the communications industry. This is how we at the Commission get things right: by bringing people from inside and outside the Commission who have each engaged in different parts of the communications ecosystem.<sup>14</sup>

The cable industry is committed to the public-private partnership model embodied by CSRIC as one of several forums for addressing cyber security. Comcast, Time Warner Cable, and Cox representatives serve on the CSRIC full committee, including Glenn A. Britt, Chairman, President and CEO, Time Warner Cable; Patrick Esser, President, Cox Communications; and John Schanz, Executive Vice President, National Engineering & Technology Operations, Comcast Corporation.<sup>15</sup> Cable representatives are also active members of the CSRIC working groups, including those addressing cyber security issues.<sup>16</sup>

---

<sup>12</sup> See FCC, *CSRIC Working Group Descriptions, Working Group 2A – Cyber Security Best Practices*, available at <http://www.fcc.gov/pshs/advisory/csric/wg-2a.pdf>.

<sup>13</sup> As we recently discussed in the network survivability proceeding, CSRIC should also be key to the Commission’s approach to promoting network reliability and survivability. See NCTA Comments, *In re Effects on Broadband Communications Networks Of Damage to or Failure of Network Equipment or Severe Overload*, PS Docket No. 10-92, at 14-16 (June 25, 2010) (“*NCTA Survivability Comments*”).

<sup>14</sup> Julius Genachowski, Chairman, FCC, Remarks at the Communications Security, Reliability & Interoperability Council Meeting, Washington, D.C: Strengthening Public Safety Infrastructure and Emergency Response Capabilities 2 (Dec. 7, 2009), available at <http://www.fcc.gov/pshs/advisory/csric/chairman-remarks.pdf>.

<sup>15</sup> See FCC, *Communications Security, Reliability & Interoperability Council (CSRIC) Members*, at <http://www.fcc.gov/pshs/advisory/csric/members.html> (last visited July 6, 2010); see also NCTA *Cyber Security Comments* at 7-8.

<sup>16</sup> See FCC, *Working Group 2A – Cyber Security Best Practices* (noting, for example, that Myrna Soto, Comcast Corporation, is one of the co-chairs of the 24-member cyber security working group), at <http://www.fcc.gov/pshs/advisory/csric/wg-2a-members.pdf> (last visited July 7, 2010); see also NCTA *Survivability Comments* at 15.

The cable industry is also active in a number of other federal and non-federal initiatives that are addressing cyber security policies and practices. As we previously described in comments in the National Broadband Plan proceeding, the cable industry is involved in the National Security and Telecommunications Advisory Committee (“NSTAC”), the National Communications Center (“NCC”), and the Communications Sector Coordinating Council (“CSCC”).<sup>17</sup> Cable industry engineers in network operations and management also participate in the Messaging Anti-Abuse Working Group (MAAWG)<sup>18</sup> and the Quality and Reliability Committee of the Institute for Electrical and Electronics Engineers (IEEE). In addition, there are several cable-specific working groups and activities in this area led by the Society of Cable Telecommunications Engineers (“SCTE”)<sup>19</sup> and Cable Television Laboratories, Inc.

But cable operators and other Internet Service Providers are hardly the only entities with interests in and responsibilities for ensuring cyber security. CSRIC and other coordinated efforts should develop best practices not only for “last mile” networks, but for other key sectors of the Internet ecosystem. The Commission appears focused on “Internet service providers,”<sup>20</sup> but today’s Internet is characterized by a complex web of entities providing a wide array of interrelated functions. Limiting its inquiry to Internet Service Providers would be myopic and ineffective. Indeed, while the Commission seeks to protect the “broadband communications”

---

<sup>17</sup> See *NCTA Cyber Security Comments* at 6-7; see also *NCTA Survivability Comments* at 12-16 (describing the cable industry’s involvement in a number of efforts, including those underway at the U.S. Department of Homeland Security).

<sup>18</sup> See MAAWG, *Member Roster*, at <http://www.maawg.org/about/roster> (last visited July 12, 2010). MAAWG is an industry group developing methodologies to protect consumers from spam, phishing, and fraudulent emails, and to improve online safety. MAAWG sponsors include Comcast, Cox, and Time Warner Cable, as well as many other Internet Service Providers and entities such as AOL, Facebook, Google, and Yahoo!.

<sup>19</sup> See *NCTA Survivability Comments* at 16.

<sup>20</sup> Notice ¶ 17.

infrastructure,<sup>21</sup> such infrastructure includes not only so-called “last mile” facilities operated by broadband access facilities, middle-mile transport, and backbone facilities operated by Internet Service Providers, but content delivery networks (“CDNs”), server farms, and services operated by “application” providers such as Google, Facebook, and Yahoo, among others. Moreover, most of the leading cyber threats today do not target the physical transmission layer. For example, cyber terrorists or hackers are much more likely to disrupt or shut down social networking, e-mail, or gain access to personal or sensitive information through phishing attacks, rather than disrupt the underlying broadband networks.<sup>22</sup> It would not benefit the public if broadband Internet access facilities remained up and running but broadband communications were halted by attacks affecting some other vulnerability in the Internet ecosystem.

The global nature of the Internet – and of threats to network survivability and continuity of service – underscore that a narrow regulatory approach focused on Internet service providers operating in the United States would be short-sighted and ineffective. China’s well-publicized interference with Google’s services, which compromised the privacy of its users’ communications, underscores this reality.<sup>23</sup> Because terrorists and foreign governments that do not respect our values can target particular applications and affect millions of users, the U.S. governmental response must apply as broadly as these potential threats.

---

<sup>21</sup> *Id.* ¶¶ 2, 4.

<sup>22</sup> *See, e.g.,* Ki Mae Heussner, *Watch Out: Cyber Threats to Expect in 2010*, ABC News/Technology, Jan. 1, 2010 (“Although consumers know to be wary of Web links sent by strangers, they tend to trust Web links and e-mail messages sent by friends and family. But online attackers are learning how to exploit that trust, by delivering malware that appears to come from Facebook friends, Twitter followers and friends’ e-mail accounts.”), at <http://abcnews.go.com/Technology/cyber-threats-expect-2010/story?id=9456824>; John Markoff, *Cyberattack on Google Said to Hit Password System*, N.Y. Times, Apr. 20, 2010 at A1 (describing cyber attack against Google).

<sup>23</sup> *See* Markoff, *supra* note 22; Ben Worthen, *Researcher Says Up to 100 Victims in Google Attack*, Wall St. J., Feb. 26, 2010, available at <http://online.wsj.com/article/SB10001424052748704625004575090111817090670.html>.

Accordingly, the Commission should broaden CSRIC's membership to include not only broadband network owners and public safety groups – who make up a significant percentage of existing members – but also backbone providers, CDNs, application providers, computer manufacturers, software developers, and others with a stake in maintaining a robust and secure Internet.

To the extent the Commission feels a need to promote compliance with the cyber security best practices formulated by CSRIC, the Commission should consider tasking CSRIC with publishing a checklist that companies can use as a tool to implement best practices. This approach has been taken in the past. For example, the Toolkit Working Group of the Media Security and Reliability Council published model vulnerability assessment checklists.<sup>24</sup> But a rigid, procedure-laden, and costly certification program is not the answer.

### **CONCLUSION**

For the foregoing reasons, the Commission should not establish a cyber security certification program.

Respectfully submitted,

**/s/ Loretta P. Polk**

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

July 12, 2010

---

<sup>24</sup> See Media Security and Reliability Council, *Local Cable System Model Vulnerability Assessment Checklist* (Nov. 16, 2004), available at <http://www.mediasecurity.org/documents/CableVulnerabilityChecklist.pdf>.