

aspects of broadband services.¹ 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.”²

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.”³ 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.”⁴

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,

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

² *Id.* at 1.

³ *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.

⁴ *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.⁵ 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.⁶

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

⁶ *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.⁷ 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

⁷ “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.⁸ 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.⁹ 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."¹⁰ 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.¹¹

⁸ *Id.*

⁹ 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/.

¹⁰ 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.

¹¹ 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.

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.¹² 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.¹³

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

¹² See e.g. 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/>.

¹³ 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.¹⁴ 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.¹⁵ 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

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

¹⁵ 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."¹⁶

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.¹⁷

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

¹⁶ 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.

¹⁷ *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.”¹⁸

Moreover, ensuring that network providers have the flexibility and tools needed to address network security is also fundamental to broadband adoption strategies.¹⁹ 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.²⁰

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.”²¹ 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

¹⁸ White House Cyberspace Policy Review Report at 31.

¹⁹ 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.

²⁰ 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.”).

²¹ 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.”²² 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.”²³

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

²² *Id.* at ¶ 140.

²³ *Id.*