

**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. Poday  
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>.