

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	PS Docket No. 10-146
)	GN Docket No. 09-51
National Broadband Plan Recommendation)	
to Create a Cybersecurity Roadmap)	DA 10-1354

**COMMENTS OF THE
NATIONAL TELECOMMUNICATIONS COOPERATIVE ASSOCIATION**

The National Telecommunications Cooperative Association (NTCA)¹ responds to the Federal Communications Commission (FCC or Commission)'s Public Safety and Homeland Security Bureau 's August 9, 2010 Public Notice (Public Notice) seeking comment on the National Broadband Plan's Recommendation No. 16.5 regarding the need for a national cybersecurity roadmap.² The Public Notice specifically asks commenters to identify: 1) the most critical cybersecurity threats to the communications infrastructure; and 2) what role the Commission should play in addressing, remediating, and coordinating efforts to address cybersecurity threats.³ The Commission anticipates completion of the cybersecurity roadmap by November 2010.⁴

Recommendation 16.5 of the National Broadband Plan directed as follows: "The country needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely. Within 180 days of the release, the FCC

¹ NTCA is a premier industry association representing rural telecommunications providers. Established in 1954 by eight rural telephone companies, today NTCA represents 585 rural rate-of-return regulated telecommunications providers. All of NTCA's members are full service rural local exchange carriers and many of its members provide wireless, cable, Internet, satellite and long distance services to their communities. Each member is a "rural telephone company" as defined in the Communications Act of 1934, as amended. NTCA's members are dedicated to providing competitive modern telecommunications services and ensuring the economic future of their rural communities.

² *FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, PS Docket No. 10-146, GN Docket No. 09-51, Public Notice, DA 10-1354 (rel. Aug. 9. 2010) (Notice).

³ *Id.* at 1, 2.

⁴ *Id.* at 2.

should issue, in coordination with the Executive Branch, a plan to address cybersecurity. The FCC roadmap should identify the five most critical cybersecurity threats to the communications infrastructure and its end users. The road map should establish a two-year plan, including milestones, for the FCC to address these threats.”⁵ Thus, the recommendation is two-fold: first, identify the cyber threats and second, create a two-year plan to “address” the threats. NTCA suggests that the Commission should focus on giving communications providers the tools, training, and resources to protect their networks and educate their customers as part of the national cybersecurity roadmap.

The first task under the National Broadband Plan (identifying cyber threats) is relatively easy to achieve. Perhaps the most severe threat is a denial of service attack, which poses the risk of overloading and shutting down interconnected communications networks. Providers must also deter and guard against hacking into switches, remote data centers used for cloud computing, and other network components. Another cyber threat is phishing, which is “attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity.”⁶ A fourth type of cyber attack is the unauthorized installation of malware and spyware, including worms, trojans, viruses, and botnets that are hidden within emails and attachments. Still another is spam, which can serve as the vehicle for conveying several of the threats described above.

The second task, creating a two-year plan to address the threats, is far more difficult to achieve. The issues are complex, the means of attack are varied, and the methods of carrying out such threats change over time. Providers such as NTCA’s small rural telco companies already have adequate market incentive to guard their networks and educate their rural customers about

⁵ Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan*, Recommendation 16.5 (rel. Mar. 2010).

⁶ Wikipedia definition, “phishing,” <http://en.wikipedia.org/wiki/Phishing>, accessed September 21, 2010.

cyber attacks. Providers protect their networks and data against electronic intrusion by installing and maintaining firewalls to limit access and by encrypting data. Providers patch and update their servers frequently to cure software vulnerabilities. Providers train their employees to prevent cyber attacks by using complex passwords and login codes. Information technology (IT) security policies are typically part of providers' procedures manuals. When a provider detects an attempt to hack into a switch or remote unit, its IT department responds by using multilayered security levels that include freezing the network temporarily, diagnosing the extent of the attack and finding its source, then recovering or restoring the data.

NTCA members already advertise cyber security services, such as computer protection packages that include anti-virus and anti-spyware protection, pop-up blockers, firewall protections, secure remote data centers, and parental controls. Others offer security set-ups, business maintenance plans, computer diagnostics, and spam filtering. NTCA member companies frequently provide round-the-clock tech support for their Internet customers. Ad blockers, junk email filtering, and links to Internet safety and cyber crime reporting agencies are also offered by NTCA members to their rural customers. NTCA members already recognize that consumer education is key to minimize the threat of electronic intrusions.

It would seem too much, however, for the Commission to attempt to identify, prevent, *and* remedy all cyber security attacks, particularly as these threats (and the networks they threaten) evolve over time. Thus, rather than considering specifically how to "remediate" such threats, the Commission's cybersecurity plan should focus primarily on what resources it can offer to educate providers, what the Commission can do to raise public/consumer awareness of such threats, and how it can assist in promoting public-private partnerships and coordinating

cybersecurity measures under consideration by various federal government entities and industry groups.

Given the short period (*i.e.*, November 2010) for completion of the cybersecurity roadmap, the Commission should focus its efforts on enabling communications providers of all types to protect their networks and to educate their customers about cyber security threats and preventative measures.

Respectfully submitted,



By: /s/ Michael Romano
Michael Romano
Senior Vice President - Policy

By: /s/ Karlen Reed
Karlen Reed
Senior Regulatory Counsel – Legal & Industry

Its Attorneys

4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203
(703) 351-2000

September 23, 2010

CERTIFICATE OF SERVICE

I, Rita H. Bolden, certify that a copy of the foregoing Comments of the National Telecommunications Cooperative Association in PS Docket No. 10-146, GN Docket No. 09-51, DA 10-1354, was served on this 23rd day of September 2010 via electronic mail to the following persons:

Julius Genachowski, Chairman
Federal Communications Commission
445 12th Street, SW, Room 8-B201
Washington, D.C. 20554
Julius.Genachowski@fcc.gov

Commissioner Michael J. Copps
Federal Communications Commission
445 12th Street, SW, Room 8-B115
Washington, D.C. 20554
Michael.Copps@fcc.gov

Commissioner Robert M. McDowell
Federal Communications Commission
445 12th Street, SW, Room 8-C302
Washington, D.C. 20554
Robert.McDowell@fcc.gov

Commissioner Mignon Clyburn
Federal Communications Commission
445 12th Street, SW, Room 8-A302
Washington, D.C. 20554
Mignon.Clyburn@fcc.gov

Commissioner Meredith Attwell Baker
Federal Communications Commission
445 12th Street, SW, Room 8-A204
Washington, D.C. 20554
Meredith.Baker@fcc.gov

Best Copy and Printing, Inc.
Federal Communications Commission
445 12th Street, SW, Room CY-B402
Washington, D.C. 20554
fcc@bcpiweb.com

Jeffery Goldthorp, Associate Chief
FCC
Public Safety & Homeland Security
445 12th Street, SW
Washington, DC 20554
Jeffery.Goldthorp@fcc.gov

/s/ Rita H. Bolden
Rita H. Bolden