



TELECOMMUNICATIONS

SNAP UPdateSM

September 7, 2010

By: Craig Dingwall

Cybersecurity Roadmap or Internet Roadblock?

As part of the FCC's National Broadband Plan ("NBP"), the FCC recently sought comments on the creation of a "Cybersecurity Roadmap" to identify vulnerabilities to communications networks and to develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks to networks.

What is cybersecurity, and why is it important? Cybersecurity essentially means protecting the Internet infrastructure and information that passes over it from security threats. As its name suggests, cybersecurity protects data and control systems designed to ensure the functioning of our critical infrastructure. Domestic and foreign bad actors have demonstrated the ability to steal, alter, or destroy data. Cybersecurity is important because customers will not use broadband services if they don't believe that they are secure. Moreover, unchecked vulnerabilities in the broadband communications infrastructure could threaten life, safety and privacy.

To address cybersecurity, the FCC in the NBP recommends 1) the creation of a nationwide interoperable public safety wireless broadband communications network, 2) surveying public safety broadband wireless infrastructure and devices, 3) ensuring that broadband satellite service is part of any emergency preparedness program, and 4) preserving broadband communications during emergencies. The FCC in the NBP asked Congress to consider providing funding of \$3.75 million per year for three years (for a total of \$11.3 million) to allow FEMA to expand its data collection and survey efforts with states and territories.

One of the critical challenges to cybersecurity is lack of access to broadband services. For

SNAP UPdate is a free service of Technology Law Group
A complete set of SNAP UPdates can be accessed at our website, tlgdc.com
© TLG 2008

If you would like to be removed from our email list, please notify us at
mail@tlgdc.com

example, some Public Service Access Points (“PSAPs”) are located in areas where broadband communications are unavailable, and many PSAPs cannot afford broadband connectivity. Further, regulatory roadblocks have hindered next generation, so called NG911, which will enable the public to access 911 through text messaging (SMS) and other formats.

Through the Cybersecurity Roadmap, the FCC seeks to address vulnerabilities to core Internet protocols and technologies and threats to end-users, including consumers, businesses and public safety. The FCC anticipates completion of the Cybersecurity Roadmap by November 2010. The FCC raised the following questions for public comments:

- What are the most vital cybersecurity vulnerabilities for communications networks or users?
- How can these vulnerabilities be addressed? What role should the FCC play in addressing them?
- What steps should the FCC take, if any, to remediate them?
- If the FCC does not play a role in addressing these vulnerabilities and problems, what agency or entity would fill that role?
- How should the FCC coordinate its efforts with other agencies of government?

Is a Cybersecurity Roadmap a worthwhile? Is it worth the cost? Will it address the FCC’s goals of addressing vulnerabilities to core Internet protocols and technologies, as well as threats to end-users? Can it keep up with technology changes? Will it saddle the Internet and broadband with unnecessary regulations? Have all the necessary players been identified and involved to make this work? We welcome your thoughts. Feel free to comment at our interactive blog at blog.tlgdc.com!

Field Code Changed

Comments are due September 23, 2010.

If you have questions about this issue, or if we may be of assistance to you, please feel free to contact us.

© 2010 Technology Law Group. Craig Dingwall is an attorney with the Technology Law Group, a Washington, D.C.-based law firm specializing in telecommunications transactional matters, complex litigation and intellectual property issues. Craig can be reached at cdingwall@tlgdc.com, at 202-895-1707, or at our website: www.tlgdc.com. The views in this article are those of the author, and do not necessary represent those of the Technology Law Group.

To opt out of any resource that you have previously signed up for, please click [Opt Out](#) and provide us with your email address and the resource(s) that you no longer wish to receive.