



KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

September 23, 2010

The Center for Democracy & Technology (“CDT”) respectfully submits these comments in response to the Federal Communications Commission’s (“FCC’s”) Public Notice No. 10-146, seeking public comment on the National Broadband Plan Cybersecurity Roadmap (“the Roadmap”). CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet. CDT has been actively involved in the Congressional and Executive Branch consideration of cybersecurity issues, and has testified before both the House and Senate on this topic.

I. Introduction

The Internet is a powerful engine for driving economic opportunity, increasing the efficiency of industry, broadening the exercise of free speech, and promoting civic engagement in government. In order for these benefits to be fully realized, however, the Internet must be reasonably secure against threats posed by malicious traffic. Government cybersecurity policies are one important tool capable of promoting an appropriate level of security.

This Public Notice asked for comments on the most dangerous cybersecurity vulnerabilities for networks and users, as well as suggestions as to how best to ameliorate those vulnerabilities. It then specifically focused on several questions surrounding the role of the FCC in addressing these issues, asking what steps the FCC should take and how it should coordinate its efforts with other agencies and entities. These comments address this second set of more focused questions.

CDT believes that the FCC should recognize that a significant number of other federal agencies are working to secure networks in both the public and private sectors, including public and private communications infrastructure. In order to reduce potential conflicts with these other agencies, we believe that the Roadmap should embrace three guiding principles: limited authority, consultation, and transparency.

II. Three Guiding Principles

The FCC Should Not Take a Major Role in Securing Private Networks – In order to safeguard an open and unregulated Internet, CDT has consistently argued that the Commission lacks open-ended jurisdiction over Internet communications, and that where it does have some jurisdiction it should assert only a narrow and focused basis for jurisdiction.¹ Any broad-based assertion of regulatory power over the diverse set of

¹ See *Comments of the Center for Democracy & Technology In the Matter of Framework for Broadband Internet Service*, GN Docket No. 10-127, July 15, 2010, www.cdt.org/files/pdfs/CDT_Comments-Framework_for_Broadband.pdf; *Comments of the Center for Democracy & Technology In the Matter of Preserving the Open Internet: Broadband Industry Practices*, GN Docket No. 09-191, January 14, 2010, http://www.cdt.org/files/pdfs/2010_CDT_openness_comments.pdf.

actors in the Internet ecosystem would ultimately threaten the low barriers to entry for new Internet-based businesses and risk reducing the openness of the network. The risk raised by broad assertion of FCC authority is exacerbated by the multiplicity of Federal entities addressing cybersecurity. Several other executive branch agencies already exercise some degree of authority over the protection of private sector networks, including the Department of Homeland Security (DHS), the White House Office of the Cybersecurity Coordinator, and the Department of Commerce.

Absent a clear Congressional mandate, the FCC should circumscribe its own cybersecurity activities so as not to add additional burdensome oversight in the name of minimal gains in cybersecurity. Moreover, the Commission, to the extent that it does take actions in the area of cybersecurity, should do so only with regard to entities (such as telecommunications carriers) over which the Commission has clear authority. The FCC does have a clear and valuable role in cybersecurity that includes maintaining law enforcement access to communications under the Communications Assistance to Law Enforcement Act (CALEA) and ensuring the continued operations of emergency services under the Enhance 911 Act. The Commission should continue to pursue its work in such areas, but in light of the responsibilities allocated to DHS, it should not seek to play a central or leading role in cybersecurity.

The FCC Should Consult With the Private Sector and Other Federal Actors Before Taking Any Regulatory Action – Given the possibility of over-regulation by the assorted federal actors named above, the FCC should consult with industry, the White House, and DHS before taking on cybersecurity responsibilities as part of the Roadmap. By consulting with other federal agencies, the FCC can reduce potential policy conflicts and redundant actions. With regard to entities over which the Commission has jurisdiction, the Commission can promote best practices and standards in collaboration with public/private bodies rather than through government-run regulatory processes. The FCC can thereby ensure that its cybersecurity efforts are aimed at the limited set of concerns that the private sector may not be adequately able to address on its own.

The FCC already convenes one such advisory group: the Communications Security, Reliability and Interoperability Council (CSRIC). The FCC should work with DHS and the White House to determine whether CSRIC or a similar group can serve a valuable role in addressing cybersecurity concerns, and how to deconflict that role from those played by other public/private collaborative bodies such as the National Security Telecommunications Advisory Committee, the National Coordinating Center for Telecommunications, and the Information Technology Information Sharing and Analysis Center.

Any FCC Action Should Be Transparent to Consumers and Industry – Any actions that the FCC considers should be transparent to both consumers and industry. Disclosure of information by carriers to the FCC should, within reason, be shared with the public in order to maximize consumer access to information about the broadband service marketplace. Any effort to develop best practices should be made through an open process permitting both comment and participation from industry and outside experts, so that the resulting best practices are well understood by all stakeholders.

III. Conclusion

CDT believes that maintaining the security of both public and private communications infrastructure is critical, in no small part because it serves the goal of maintaining an open, innovative and free Internet. The FCC can best serve both security and openness by taking a limited role in cybersecurity, adopting transparent processes, and committing to continued consultation with the public and private sectors.

Respectfully submitted,

Greg Nojeim
Joshua Gruenspecht
Center for Democracy and Technology
1634 I Street, NW
Suite 1100
Washington, DC 20006
202-637-9800
