Gen Docket No 09-51

Gregory Intoccia

From: Jennifer Manner
Sent: Tuesday, October 20, 2009 11:07 AM
To: Gregory Intoccia; Jeffery Goldthorp; Richard Hovey; Gregory Cooke; Jean Ann Collins
Cc: Ronnie Cho
Subject: FW: Blog

FILED/ACCEPTED
SEP 30 2009
Federal Communications Commission
Office of the Secretary

FYI.

From: Ronnie Cho
Sent: Tuesday, October 20, 2009 10:00 AM
To: Jennifer Manner
Subject: Blog

Hey Jennifer,

Here is a comment from the cyber security blog.

http://blog.broadband.gov/?p=587#comments

Also, I sent Gray the youtube clip of the President talking about "cyber security month" and will let you know when it goes up.

No. of Copies rec'd 2
List ABCDE

« A National Broadband Clearinghouse Low Country Broadband »

Cyber Security

October 16th 2009 by Jamie Barnett

The recent Cyber Security Broadband Workshop was a fascinating discussion, featuring panelists from a diverse group of backgrounds and perspectives. We explored solutions and discussed many of the challenges that government and the private sector face in achieving cyber security as a matter of public safety and economic security. So much of our lives rely on the Internet and the need to secure our online infrastructure is critically important, so I want to highlight just a few take-aways from the workshop. The experts agree that cyber security is not a barrier to broadband deployment, but methods of prevention, detection and restoration must continually be developed. The public must have knowledge of what cyber attacks are and where they may come from and stay alert. We all must do our part. As technologies get more sophisticated, so do the threats.

Our panelists acknowledged the need to expand cyber security awareness and education for consumers and provide user friendly tools and best practices to help protect personal computers. Dr. Don Welch noted that the return on investment for cyber security, for both private and public entities, is negative: in other words, all the money and resources spent to protect systems go to ensuring that nothing happens. The business community and government face the challenge of implementing robust cyber security solutions without severely stifling innovation or devalue the user experience. These were just a few interesting items of discussion from a conversation I hope we continue to have as the broadband plan is developed. A key measure of our success in this area will be the degree to which we help increase the American public's knowledge and awareness of cyber security and the actions they can take to protect themselves and their privacy. Please feel free to contribute to the on-going conversation by sharing your comments and questions. In case you missed the workshop, you can view the presentations and materials here.

4 Responses to "Cyber Security"

Jim Lippard says:
10/16/2009 at 11:29 AM

"Dr. Don Welch noted that the return on investment for cyber security, for both private and public entities, is negative; in other words, all the money and resources spent to protect systems go to ensuring that nothing happens."

That seems to me to be an incorrect way of measuring under which all investment in infrastructure has negative ROI. Security is part of an infrastructure that *enables* delivery of services in a robust, reliable way, by guaranteeing some degree of confidentiality, integrity, and availability.

If security has negative ROI under this argument, so does redundancy and resiliency. But nobody argues that standard features of datacenter buildouts like redundant power and bandwidth has negative ROI, do they?

Johannes de Haas says:
10/18/2009 at 9:17 PM

Isnt Cybersecurity the jurisdiction of DHS???

Tony Rutkowski says:
10/19/2009 at 4:15 PM

How can one credibly assert that "A key measure of our success in this area will be the degree to which we help increase the American public's knowledge and awareness of cyber security and the actions they can take to protect themselves and their privacy." That's a measure of doing nothing.

The Commission needs to take steps to "bake" cybersecurity into the infrastructure by implementing an array of security and identity management requirements that all providers must implement, and do it together with other nations who are facing the same cyhersecurity crisis. As to what must be done, the Commission can begin using the new Cybersecurity Command to provide the specifics of what must be done.

Daniel Puroclean says:
10/28/2009 at 5:51 PM

Hi Jamie, if all the money and resources spent to protect systems go to ensuring that nothing happens, as Dr. Don Welch states, then how do you measure success? How do you know that things are heading along the right path and systems are being protected vs. no one having tried yet to

breach that system?