



November 5, 2010

Via ECFS  
Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 Twelfth Street, SW  
Washington, DC 20554

Re: Notice of Ex Parte Presentation: Public Notice, FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap (PS Docket No. 10-146 and GN Docket No. 09-51); Cyber Security Certification Program (PS Docket 10-93); Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment Or Severe Overload (PS Docket No. 10-92)

Dear Ms. Dortch:

On November 3, 2010, Adam Golodner, Director, Government Affairs, Don Proctor, Senior Vice President in the Office of the Chairman of the Board and Chief Executive Officer, and the undersigned met with the following Public Safety and Homeland Security Bureau officials to discuss various issues in the above-captioned dockets: James Arden Barnett, Jr. Chief, Jennifer Manner, Deputy Chief, Jeffrey Goldthorp, Associate Chief, and Lisa Fowlkes, Deputy Chief. The purpose of the meeting was to discuss the FCC's pending cybersecurity roadmap and to learn Cisco's views of the likely topics of focus for the roadmap.

The focus of the conversation was DNSSEC and border gateway protocol technology. Cisco noted its heavy involvement in DNSSEC through ICAAN and IETF, and stated that the information available to us indicates the DNSSEC pilot now underway is going well. Cisco stated its view that the right first steps are deployment of DNSSEC within the root, and that with DNSSEC deployment already in motion, perhaps the FCC could encourage next steps through ISP "best practices." On border gateway protocol technology, Cisco noted that work is ongoing on both origin, validation and path security, and that the IETF is actively considering approaches to these issues. Cisco reiterated its view that industry players have implemented "best practices" that have protected networks thus far, and that while additional technical and standards work continues, the FCC may wish to focus its Communications Security, Reliability and Interoperability Council (CSRIC) on collecting those best practices. In response to staff inquiries, Cisco also said that to the extent the FCC wants to measure actual implementation of BGP standards or DNSSEC, the CSRIC could again be of use.

As it had in a prior meeting, Cisco noted that from a global perspective, that the FCC's initiatives in cybersecurity need to highlight the important role of public-private partnerships, extensive trust relationships between the market and government participants, and the aligned

incentives of the public sector and the IT and IT dependant industries to continue to drive trust across networks. In contrast, where governments elsewhere in the world deviate from the use of international standards, best-practices, and public-private partnerships, those divergent government directed actions tend to pull apart interoperability and security, lead toward a balkanization of the Internet, and retard the growth of the global benefits from a robust interconnected network. Cisco has consistently pointed to the US process, with its heavy reliance on public private partnerships, as a model for what the rest of the world should use in addressing cyber security issues.

Sincerely,



Mary L. Brown  
Director, Government Affairs

CC:  
Jennifer Manner  
Lisa Fowlkes  
Jeff Goldthorp