

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

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

**COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.**

Craig J. Brown  
Lawrence E. Sarjeant  
Suite 950  
607 14<sup>th</sup> Street, N.W.  
Washington, DC 20005  
202-429-3112  
[Craig.brown@qwest.com](mailto:Craig.brown@qwest.com)  
[Lawrence.sarjeant@qwest.com](mailto:Lawrence.sarjeant@qwest.com)

Attorneys for

QWEST COMMUNICATIONS  
INTERNATIONAL INC.

September 23, 2010

## TABLE OF CONTENTS

	Page
I. INTRODUCTION AND SUMMARY .....	1
II. DISCUSSION.....	2
A. There Is A Need For A Unified Federal Cyber Security Policy.....	2
B. The Commission Can Have A Beneficial Impact On Cyber Security By Addressing Cyber Security At The Edges Of Communications Networks. ....	6
C. Qwest’s Consumer Internet Protection Program .....	9
III. CONCLUSION.....	10

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

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

**COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.**

Qwest Communications International Inc. (Qwest), through counsel and in response to the Federal Communications Commission's (Commission or FCC) *Public Notice* released on August 9, 2010,<sup>1</sup> files these comments.

**I. INTRODUCTION AND SUMMARY.**

The Commission has asked for comment “on the creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and to develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks in coordination with federal partners.”<sup>2</sup> The request is based upon Recommendation 16.5 of the National Broadband Plan (NBP), which recommends that the Commission issue, “in coordination with the Executive Branch, a roadmap to address cybersecurity.”<sup>3</sup> Recommendation 16.5 concludes that the United States “needs a clear strategy for securing the

---

<sup>1</sup> Public Notice, DA 10-1354, *FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, rel. Aug. 9, 2010.

<sup>2</sup> *Id.* at 1.

<sup>3</sup> Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan* (March 2010) at 321 (Recommendation 16.5).

vital communications networks upon which critical infrastructure and public communications rely.”<sup>4</sup>

A Cybersecurity Roadmap developed solely by the Commission will not materially improve core network security from cyber attacks and could prove to be counter-productive. Any initiative undertaken by the Commission to address cyber security in core communications networks should operate as a public-private partnership and be coordinated with the cyber security activities of other Federal agencies.

End user adoption of available cyber protection mechanisms and security practices is currently low. Qwest has demonstrated that assisting customers in ridding their computers of infections and educating them about safe Internet security practices not only improves the online experience of individual customers but also the experiences of broad segments of the online community. The Commission should, therefore, focus its attention and resources on cyber security at the edges of communications networks through end user-targeted cyber assistance and education programs.

## II. DISCUSSION

### A. There Is A Need For A Unified Federal Cyber Security Policy.

Qwest believes that the nation has a compelling need for a uniform, strategic cyber security plan. It is a point that was emphasized in the comprehensive cyber security policy review conducted at the direction of President Obama shortly after his election.<sup>5</sup> The need for a comprehensive national cyber security plan that brings a coordinated and centralized focus to the

---

<sup>4</sup> *Id.*

<sup>5</sup> See *CYBERSPACE POLICY REVIEW, Assuring a Trusted and Resilient Information and Communications Infrastructure (Cyberspace Policy Review)* (White House, May 2009). “Prepare for the President’s approval an updated national strategy to secure the information and communications infrastructure.” Table 1: Near-Term Action Plan at vi.

Federal government's activities in this area is also the driving force behind ongoing House and Senate legislative efforts to adopt comprehensive cyber security legislation that would strengthen the nation's cyber security posture.<sup>6</sup> Qwest is concerned, though, that a Commission-developed Cybersecurity Roadmap to address the most critical cyber security threats to communications networks, however well-intentioned, will duplicate or conflict with the cyber security activities of other Federal agencies that are focused on critical communications infrastructures. Qwest is particularly concerned that a Commission-adopted action plan with milestones for "countermeasures and solutions in preparation for, and response to, cyber threats and attacks"<sup>7</sup> cannot be successfully executed without the full participation of, or coordination with, other Federal agencies that have already engaged the communications and information technology (IT) sectors in critical communications infrastructure protection planning and activities.<sup>8</sup> Although the *Public Notice* states that completion of the Cybersecurity Roadmap is anticipated by November 2010<sup>9</sup> and a Commission official is reported to have said that he expects the release of the Cybersecurity Roadmap early in 2011,<sup>10</sup> the *Public Notice* is silent on what coordination with

---

<sup>6</sup> Among the major cyber security bills introduced in the current Congress are: the Cybersecurity Act of 2010, S. 773; the Protecting Cyberspace As A National Asset Act of 2010, S. 3480; the Cybersecurity Enhancement Act, H.R. 4061; and the Protecting Cyberspace As A National Asset Act of 2010, H.R. 5548.

<sup>7</sup> *Public Notice* at 1.

<sup>8</sup> On this point, the following observation in the *Cyberspace Policy Review* is noteworthy: "The Federal government is not organized to address this growing problem [intrusions that threaten to damage portions of our critical infrastructure] effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. The government needs to integrate competing interests to derive a holistic vision and plan to address the cybersecurity-related issues confronting the United States." *Cyberspace Policy Review*, Preface at i.

<sup>9</sup> *Public Notice* at 2.

<sup>10</sup> See TRDAILY, September 20, 2010, *FCC OFFICIAL SEES CYBERSECURITY ROAD MAP RELEASED IN EARLY 2011*, <http://www.tr.com/online/trd/2010/td092010/index.htm>.

Federal partners or the Executive Branch has occurred to date or is contemplated by the Commission before its completion.

As the Government Accountability Office (GAO) noted in a recent report to Congress concerning critical infrastructure protection (CIP),<sup>11</sup> the Department of Homeland Security (DHS) has, as a part of its responsibility, issued a national infrastructure protection plan (NIPP) which was updated in 2009.<sup>12</sup> “The NIPP is intended to provide the framework for a coordinated national approach to address the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation’s critical infrastructure. The NIPP relies on a sector partnership model as the primary means of coordinating government and private sector CIP efforts.”<sup>13</sup> Federal agencies are assigned specific industry sector responsibilities relative to CIP. The communications and IT sectors are assigned to DHS.<sup>14</sup> Among the specific initiatives undertaken by DHS with respect to cyber security and the communications sector is leading an inter-agency review of the National Cyber Incident Response Plan (NCIRP).<sup>15</sup>

The Commission asks: what role it should play, if any, in addressing vital cyber security vulnerabilities for communications networks; what agency should play a role in addressing these vulnerabilities if it is not the Commission; and how the Commission should coordinate its efforts with other government agencies.<sup>16</sup> As Qwest has stated in recent comments filed with the

---

<sup>11</sup> Government Accountability Office Report to Congressional Requesters, **CRITICAL INFRASTRUCTURE PROTECTION, Key Private and Public Cyber Expectations Need to Be Consistently Addressed**, GAO-10-628, July 2010 (GAO Critical Infrastructure Protection Report).

<sup>12</sup> *Id.* at 9.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* Table 3: Sector-Specific Agencies and Assigned Sectors at 7.

<sup>15</sup> Qwest anticipates that the Commission will have a role in the implementation of the NCIRP.

<sup>16</sup> *Public Notice* at 2.

Commission in other dockets concerning cyber security and broadband network survivability, broadband network services providers and Internet services providers (ISPs) operate in a highly competitive communications market. Accordingly, they have a strong economic incentive to maintain the physical and cyber security of their core networks in order to satisfy customer expectations and protect and grow their revenues.<sup>17</sup> The imposition by the Commission of a regulatory or compliance-based program for addressing cyber security in core communications networks will not produce materially greater network security and could prove to be counter-productive. Any action taken by the Commission to address cyber security in core communications networks should employ the public-private partnership model that is the foundation of the NIPP<sup>18</sup> and be coordinated with the cyber security activities of other Federal agencies.

DHS has developed the National Cybersecurity and Communication Integration Center (NCCIC) as a centralized location for federal entities and private sector organizations to coordinate efforts to address cyber threats and respond to cyber attacks. GAO found that NCCIC “is still in development and does not currently have representation from all relevant federal agencies and private entities as envisioned”<sup>19</sup> and recommended that efforts be bolstered to build out the NCCIC as the “focal point for leveraging and integrating the capabilities of the private sector, civilian government, law enforcement, the military, and the intelligence community.”<sup>20</sup> While there may be additional agencies that the Commission should coordinate with in the area

---

<sup>17</sup> See Comments of Qwest Communications International Inc., PS Docket No. 10-93, filed July 12, 2010 (Qwest Cyber Security Certification Program Comments) at 11 and Comments of Qwest Communications International Inc., PS Docket No. 10-92, filed June 25, 2010 (Qwest Broadband Networks Survivability Comments) at 2-3.

<sup>18</sup> GAO Critical Infrastructure Protection Report at 9-11.

<sup>19</sup> *Id.* at 19.

<sup>20</sup> *Id.* at 24.

of cyber security relative to the communications and IT sectors, it should closely coordinate with DHS. The Commission should consider maintaining a high level of visibility in the NCCIC and provide whatever assistance it can to increase agency and private sector representation. The Commission should also determine, before proceeding beyond the *Public Notice*, whether there is a need for a FCC Cybersecurity Roadmap outside of the framework of the NIPP, especially in light of ongoing initiatives at DHS like the NCIRP.

**B. The Commission Can Have A Beneficial Impact On Cyber Security By Addressing Cyber Security At The Edges Of Communications Networks.**

Qwest and numerous other broadband network services providers and ISPs have submitted comments in Commission proceedings concerning the state of survivability of broadband networks and cyber security documenting that the nation's core broadband networks are sound and secure and describing the many strategies, processes and techniques that they employ to respond to, and protect against, physical and cyber attacks on their networks.<sup>21</sup> In Section II.A. above, Qwest describes just a few of the ongoing cyber security initiatives of DHS in which broadband network services providers and ISPs such as Qwest participate.<sup>22</sup> There is, of course, room for improvement in the cyber security efforts that have been undertaken to date. For example, the Federal government is the largest customer in the nation for communications and Internet services, and it could create powerful market-based incentives for broadband

---

<sup>21</sup> See generally, the comments and reply comments filed by broadband network services providers and ISPs in PS Docket No. 10-92, *In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, and PS Docket No. 10-93, *In the Matter of Cyber Security Certification Program*. See Qwest Cyber Security Certification Program Comments at 8-11; Comments of AT&T Inc., PS Docket No. 10-93, filed July 12, 2010 at 8-16 (erratum filed July 13, 2010); Comments of Verizon and Verizon Wireless, PS Docket No. 10-93, filed July 12, 2010 at 2-8; and Qwest Broadband Networks Survivability Comments at 2-3.

<sup>22</sup> In the Attachment to its Qwest Network Survivability Comments, Qwest lists more than two dozen public-private partnerships and industry organizations that are considering physical and cyber network security.

network services providers and ISPs to further increase the cyber security of their networks through its procurement practices. The Federal government could also manage its computer networks in a manner that showcase best practices that other network owners and operators could employ. As noted in the *Cyberspace Policy Review*, “federal leadership and accountability for cyber security should be strengthened. This approach requires clarifying the cyber security-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions.”<sup>23</sup> Legislation is likely required in order to facilitate such improvements. The Commission’s inability to reach across all Federal entities to drive the needed streamlining and centralization of the Federal government’s cyber security initiatives places severe constraints on a Commission-adopted Cybersecurity Roadmap to holistically address identified vulnerabilities to the nation’s core communications networks or core Internet protocols and technologies.

Although the ability of the Commission to address identified vulnerabilities in core communications networks is constrained, its ability to have a significant, positive impact on the online experiences of consumers and other end users at the edges of core communications networks through a cyber education and assistance campaign is not similarly limited. There is a compelling need for more end user cyber education and assistance. End user adoption of available cyber protection mechanisms and security practices is currently low, and this has created an opportune environment for the exploitation of Internet users by criminals and others interested in disrupting critical Internet-based activities.<sup>24</sup> The SysAdmin, Audit, Network,

---

<sup>23</sup> *Cyberspace Policy Review* at iii.

<sup>24</sup> In its updated version of the *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*, the Center for Strategic and International Studies, a nonprofit that conducts research and analysis and provides policy solutions to decision-makers in governmental and non-governmental organizations, states at 11: “Many criminal groups and nation states deploy

Security (SANS) Institute<sup>25</sup> has identified “Top Cyber Security Risks” and determined that the number one priority for addressing cyber security should be fixing “client-side software that remains unpatched.”<sup>26</sup> The number two priority identified by the SANS Institute is attending to “Internet-facing web sites that are vulnerable.”<sup>27</sup>

The Commission’s knowledge of the day-to-day workings of the communications industry places it in an ideal position to make a major contribution in educating consumer and business end users on how to best protect themselves and their organizations from cyber attacks and to provide assistance where end users have been victimized. While Qwest would encourage the Commission to leverage existing governmental and private sector cyber education and assistance initiatives, the Commission could also partner with broadband network services providers and ISPs, or work through its own Consumer and Governmental Affairs Bureau, to conduct an effective campaign.<sup>28</sup>

---

systems that continuously scan address spaces of target organizations waiting for new, unprotected systems to be attached to the network. The attackers also look for laptops not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates until the following day. Attackers from anywhere in the world may quickly find and exploit such systems that are Internet-accessible.”  
[http://csis.org/files/publication/Twenty\\_Critical\\_Controls\\_for\\_Effective\\_Cyber\\_Defense\\_CAG.pdf](http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf).

<sup>25</sup> The SANS Institute is a cooperative research company and operator of the Internet Storm Center. See <http://www.sans.org>.

<sup>26</sup> <http://www.sans.org/top-cyber-security-risks/summary.php>.

<sup>27</sup> *Id.*

<sup>28</sup> See the *Ex Parte* of Verizon filed in this proceeding on September 14, 2010, and the Comments of AT&T filed in PS Docket No. 10-93 on July 12, 2010 at 25-28 encouraging Commission involvement in consumer education on cyber security.

### **C. Qwest's Consumer Internet Protection Program**

Internet security is a high priority for Internet users and for Qwest. Most people do not know when their computers become infected. One of Qwest's goals as a provider of broadband and Internet services is to help its customers get rid of virus and malware (malicious software) infections and provide them with sufficient information to maintain strong levels of Internet security. The proliferation of cyber crime requires individuals, businesses and governmental entities to take action against ever-changing methods of attack. Viruses and malware can cause problems not only for individual customers, but also for broad segments of the online community.

Qwest has implemented a program designed to help curtail the spread of viruses and malware on the Internet and to assist its customers whose computers are infected with them. Qwest's Consumer Internet Protection Program (CIPP) notifies Qwest broadband customers about viruses and malware that may be on their computers, educates them concerning safe Internet security practices and helps them clean viruses and malware from their computers. The CIPP is part of Qwest's ongoing effort to make the Internet safer for its customers. The program is available, at no additional charge, to residential and small-business customers that subscribe to Qwest's Broadband Digital Subscriber Line (Broadband DSL) service.

Qwest monitors its network to manage it and to detect viruses and malware. Under the CIPP, Qwest also relies on information about malicious activity provided to it by third parties. When Qwest receives a report of or discovers such activity, Qwest notifies the specific Broadband DSL customer of the infection; gives the customer information on how to remove the infection; educates the customer on good Internet security practices; and provides the customer with additional resources, including downloadable or online anti-virus software.

Qwest Broadband customers have responded positively to the CIPP.<sup>29</sup> More than three-quarters of infected customers who were surveyed responded positively to the assistance received from Qwest to help them get rid of viruses and/or malware on their computers. In addition to employing CIPP, Qwest educates its customers as to proactive things they can do to remain protected online such as:

Run anti-virus software on every computer; make sure the software and virus signatures are up to date.

Periodically run anti-spyware software on all computers.

Make sure there's an up-to-date firewall operating on each computer and on broadband Internet modems.

Ensure computers run a supported operating system and have the latest operating system and application patches installed.

Use passwords and strong encryption on wireless (WiFi) access points to ensure networks are secure.

### **III. CONCLUSION**

Multiple Federal agencies are engaged in cyber security activities concerning the nation's communications infrastructure. As noted in the *Cyberspace Policy Review*, none of the agencies has sufficient decision-making authority to develop a holistic cyber security plan or direct actions that deal with cyber security issues in a consistent way. Accordingly, cooperation and coordination among Federal agencies with respect to their cyber security activities is essential if successful countermeasures and solutions in response to cyber threats are to be instituted. Before proceeding beyond the *Public Notice*, the Commission should determine whether there is a need for a FCC Cybersecurity Roadmap outside of the framework of DHS's NIPP. Should the

---

<sup>29</sup> Qwest is very pleased with its customers' positive response to the CIPP. The CIPP has also been beneficial for Qwest. It has decreased the number of customer service calls received attributable to virus and malware infections and thereby lowered Qwest's costs. Nonetheless, Qwest believes that the decision to implement a program like the CIPP should be left to individual service providers and not mandated.

Commission proceed with the creation of a Cybersecurity Roadmap, the focus of that Cybersecurity Roadmap should be improving cyber security at the edges of communications networks through end-user assistance and education programs.

Respectfully submitted,

QWEST COMMUNICATIONS  
INTERNATIONAL INC.

By: /s/ Lawrence E. Sarjeant  
Craig J. Brown  
Lawrence E. Sarjeant  
Suite 950  
607 14<sup>th</sup> Street, N.W.  
Washington, DC 20005  
202-429-3112  
Craig.brown@qwest.com  
Lawrence.sarjeant@qwest.com

September 23, 2010

CERTIFICATE OF SERVICE

I, Richard Grozier, do hereby certify that I have caused the foregoing **COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.** to be: 1) filed with the FCC via its Electronic Comment Filing System in PS Docket No. 10-146 and GN Docket No. 09-51; and 2) served via e-mail on the FCC's duplicating contractor, Best Copy and Printing, Inc. at [fcc@bcpiweb.com](mailto:fcc@bcpiweb.com).

/s/Richard Grozier

September 23, 2010