

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

---

In the Matter of:

Cyber Security Roadmap

---

)  
)  
) PS Docket No. 10-146  
) GN Docket No. 09-51  
)  
)

**COMMENTS OF AT&T INC.**

Robert Vitanza  
Gary L. Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20th Street, N.W.  
Washington, DC 20036  
(202) 457-3076  
*Counsel for AT&T Inc.*

September 23, 2010

## TABLE OF CONTENTS

	<b>Page</b>
I. SUMMARY .....	1
II. DISCUSSION.....	4
A. The Greatest Cyber Security Vulnerabilities Occur in Operating Systems and Applications and Among End Users .....	4
B. The Commission Can Play a Valuable Role in Combating Cyber Threats .....	7
1. The Commission Can Educate Consumers Regarding Responsible Cyber Security Practices .....	7
2. The Commission Should Advise and Assist Other Federal and International Cyber Security Initiatives .....	9
C. The Commission Should Not Impose Prescriptive Cyber Security Regulations on ISPs .....	10
1. Regulating ISPs Would Weaken Rather than Strengthen Cyber Security .....	10
2. The Commission Should Coordinate with Other Federal Agency Cyber Security Efforts .....	14
3. The Commission Has Not Yet Identified a Basis for Its Legal Authority over Cyber Security Issues .....	17
III. CONCLUSION.....	17

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

---

In the Matter of: )  
Cyber Security Roadmap ) PS Docket No. 10-146  
 ) GN Docket No. 09-51  
 )  
 )  
 )

---

**COMMENTS OF AT&T INC.**

AT&T Inc. (“AT&T”), on behalf of itself and its affiliates, submits these comments in response to the Federal Communications Commission’s (“Commission”) Public Notice (“Notice”) pertaining to a proposal to create a cyber security roadmap.<sup>1</sup>

**I. SUMMARY**

AT&T believes the Commission’s Notice asks the right questions about cyber security and, perhaps more importantly, the Notice does so in the right order: what are the primary cyber security vulnerabilities in the Internet ecosystem; how can they be addressed; and what role (if any) should the Commission play in addressing them. As discussed below, numerous studies have shown that the primary and most pressing cyber security vulnerabilities exist not in communications networks, but in operating systems and applications (and the devices on which they run) and among end users. Too often, operating

---

<sup>1</sup> See Cyber Security Roadmap, PS Docket No. 10-146, GN Docket No. 09-51, Public Notice, DA 10-134 (Aug. 9, 2010) (“Notice”). For more information about the nature of cyber threats facing communications networks today and some of the steps being taken to address them, AT&T refers the Commission to AT&T’s comments submitted in response to National Broadband Plan Public Notice # 8 and in response to the Cyber Security Certification Program Notice of Inquiry. See Comments of AT&T Inc., GN Docket Nos. 09-47, 09-51, 09-137 at 32-51 (filed Nov. 12, 2009) (“AT&T NBP # 8 Comments”); Comments of AT&T Inc., PS Docket No. 10-93 (filed July 12, 2010) (“AT&T Certification Program Comments”).

system providers and application developers do not incorporate adequate cyber protections into their products, and further compound the problem by not disclosing known vulnerabilities to trusted third parties who may be able to offer assistance. At the same time, end users – residential, business and government – often fail to implement the most basic precautions against malware and other threats, even though many such precautions are available at minimal, if any, cost to the user.

While these vulnerabilities are widespread, the basic solutions to many of them (though certainly not all) are within reach. First, more emphasis must be given to cyber security in the design of operating systems and applications. Although leading vendors have made strides toward more secure products in recent years, much work remains to be done in this area. Second, end users at all levels must be better educated and trained about the need to take cyber security precautions.<sup>2</sup> And they must follow through on that education and training by actually implementing such precautions.

Taken together, these two basic approaches could dramatically reduce our nation's vulnerability to cyber threats. For its part, the Commission can play a useful role in the defense against cyber attacks caused by these vulnerabilities by educating vendors and users on the nature of cyber threats and solutions to protect against them. The Commission can enhance vendors' and users' cyber intelligence by engaging them directly, through workshops or public campaigns. Indeed, during the DTV transition, the Commission demonstrated the ability to create visibility and communicate a message to a wide audience, including equipment vendors and the general population,

---

<sup>2</sup> In seeking comment solely on “vulnerabilities,” the Notice takes a purely defensive approach to cyber security. AT&T believes that effective cyber security policy must also focus on offensive strategies as well, i.e., enacting and enforcing tough laws to prevent malfeasors from launching cyber attacks in the first place. We recognize that such offensive measures are outside the Commission's bailiwick, but we would encourage the Commission to promote such measures as it coordinates with other federal agencies on cyber security policy.

on an important issue of national significance. The Commission can also engage vendors and users by coordinating its outreach efforts with other initiatives underway at other agencies to ensure a consistent, well-reinforced message from the government. And the Commission, in coordination with other relevant agencies, can work with Internet Service Providers (“ISPs”) through public/private partnerships to amplify these outreach efforts.

Given that the primary sources of cyber vulnerabilities are software and end user behavior, imposing prescriptive regulations on ISPs is not only unnecessary but would be affirmatively harmful. ISPs already have significant market-based incentives to protect their networks and customers from cyber threats. Indeed, as AT&T and others have previously explained to the Commission, ISPs currently provide a wide range of innovative security capabilities to their users. ISPs must retain the flexibility to develop and enhance these innovative approaches to quickly and decisively detect anomalies in their networks, determine whether those anomalies qualify as cyber threats, and isolate and extinguish those threats. Any regulations that prescribe the manner in which ISPs respond to these threats, or that divert ISP resources from such responses, would needlessly straitjacket ISPs in an area where maximum flexibility is critical.

Moreover, while the Commission’s interest in cyber security is laudable, by no means is the Commission the only government entity playing a role in this arena. A substantial number of Federal entities are involved in cyber security protection efforts – including the White House; the Departments of Defense, Homeland Security and Justice; the Federal Trade Commission; the National Security Agency; the Secret Service and many others – and each agency is involved in its own initiatives. The involvement of multiple Federal agencies in the cyber security effort often creates confusion and the potential for regulatory overlap, and substantial Commission regulatory involvement would only make these problems worse

(assuming the Commission properly identified its authority for such regulatory involvement in the first place). Nevertheless, the Commission's expertise with commercial communications networks and about how market-based incentives can spur innovation could prove useful in educating, advising and assisting other Federal cyber security initiatives.

## II. DISCUSSION

### A. **The Greatest Cyber Security Vulnerabilities Occur in Operating Systems and Applications and Among End Users.**

Today, a significant proportion of Internet vulnerabilities arise from the application and device layers. In its State of Software Security Report released just yesterday, Veracode reported, based upon its analysis of enterprise applications, that 57 percent of all applications fail to meet an acceptable level of security and that 81 percent of software applications supplied by third-parties fail to meet acceptable security standards.<sup>3</sup> AT&T's own experience in addressing cyber threats is consistent with Veracode's findings. AT&T's experience also shows that some vendors may hinder protection efforts by declining to share sufficient information with ISPs about known vulnerabilities in their programs until after such information becomes publicly known.

Substantial vulnerabilities also exist at the user level. Many Internet users do not take the steps necessary to protect themselves online due to cost, lack of information (or, conversely, information overload), lack of understanding, lack of interest or use of pirated software. For example, millions of users do not diligently install security patches issued by application and operating system developers. A recent paper by the Internet Security

---

<sup>3</sup> Veracode, *Executive Summary: The State of Software Security—The Intractable Problem of Insecure Software*, at 2, 3 (Sept. 22, 2010), available at <http://www.veracode.com/images/pdf/sooss/executive-summary-veracode-state-of-software-security-report-volume2.pdf>. See also AT&T Certification Program Comments at 4-7.

Alliance (“ISA”), a multi-sector trade association focused on addressing issues of information security, explained the problem: “[e]xpert testimony, including that from sophisticated government representatives, confirmed that we know how to address the vast majority of these issues, but that we are just not doing it. The key is implementation.”<sup>4</sup> The problem is exacerbated by the regular and public release of security patches. While necessary to correct security flaws, these patches can expose critical vulnerabilities to hackers, allowing them to exploit users who fail to implement the patches.<sup>5</sup>

The cyber risks arising from unsecured end-user devices are both serious and well-known to government policymakers. As the Department of Commerce recently observed:

Computing devices are highly and increasingly interconnected, meaning that security deficiencies in a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems. Put another way, poor cyber “hygiene” on one Internet-connected computer negatively impacts other connected computers.<sup>6</sup>

Indeed, one of the top ten security threat trends for 2010 identified by software security expert Symantec was the use of “social engineering as the primary attack vector.”<sup>7</sup> As Symantec explains, “more and more, attackers are going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent.”<sup>8</sup> From the perspective of the

---

<sup>4</sup> Internet Security Alliance, *Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model* at 4 (2009).

<sup>5</sup> See Mark Bowden, “The Enemy Within” *Atlantic Magazine* (June 2010) available at <http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098>.

<sup>6</sup> Cybersecurity, Innovation and the Internet Economy, Docket No.: 100721305–0305–01, *Notice of Inquiry*, 75 Fed. Reg. 44216, 44217 (July 28, 2010).

<sup>7</sup> See Kevin Haley, Symantec “Don’t Read This Blog” <http://www.symantec.com/connect/blogs/don-t-read-blog> (Nov. 17, 2009).

<sup>8</sup> *Id.*

attacker, targeting end users directly through social engineering is attractive because it can effectively bypass network- and software-based security protections without the need to exploit any systemic technical vulnerabilities.

By comparison, ISPs typically engage in substantial efforts to protect their networks and customers from cyber threats today. Although no network is completely invulnerable to cyber attacks, the comments filed in response to the Commission’s Cyber Security Certification Program Notice of Inquiry explain that ISPs have made substantial investments in equipment, services, and personnel to guard against such attacks. For example, the Alliance for Telecommunications Industry Solutions (“ATIS”) noted that “the industry’s work in the cyber security arena has been and continues to be effective.”<sup>9</sup> CTIA-The Wireless Association adds that “wireless broadband service providers have been largely successful in preventing serious cyber attacks to this point.”<sup>10</sup> Telcordia observes that “there have been considerable and successful efforts over many years by the industry and standards bodies to improve the security of broadband telecommunications, including the development of a number of valuable and applicable security criteria.”<sup>11</sup> AT&T explained that “[t]he communications industry understands the importance of cyber security to its customers and to its own economic viability, and already addresses cyber security in a substantial way.”<sup>12</sup> And in a recent report, GAO indicates that providers in the communications sector are

---

<sup>9</sup> Comments of The Alliance for Telecommunications Industry Solutions, PS Docket No. 10-93, at 5 (filed July 12, 2010) (“ATIS Comments”).

<sup>10</sup> Comments of CTIA-The Wireless Ass’n, PS Docket No. 10-93, at 2 (filed July 12, 2010).

<sup>11</sup> Comments of Telcordia Technologies, PS Docket No. 10-93, at 3-4 (filed July 12, 2010).

<sup>12</sup> AT&T Certification Program Comments at 8.

generally meeting public sector expectations for addressing cyber security issues.<sup>13</sup> It should not be surprising that ISPs effectively protect their customers and networks from cyber threats. ISPs have a strong economic incentive to maintain the security of their network infrastructure in order to protect and grow their revenues. Customers, especially business and government users, chose ISPs based upon security and reliability, among other factors. These market factors spur ISPs to innovate and to aggressively defend their networks from cyber vulnerabilities.

**B. The Commission Can Play a Valuable Role in Combating Cyber Threats.**

**1. The Commission Can Educate Consumers Regarding Responsible Cyber Security Practices.**

The Commission can positively influence the trajectory of cyber security by engaging in a comprehensive education and outreach campaign to inform consumers about security best practices and how to protect themselves and their sensitive information. As noted above, significant vulnerabilities exist and attacks can spread solely because many users neglect to take appropriate precautions to protect their devices. Indeed, according to a four-year study conducted by Verizon, 87 percent of data breaches were considered avoidable through the use of reasonable controls.<sup>14</sup> In fact, the tools for users to protect themselves are widely available, but they must be used and kept up to date in order to be effective. Unless users develop and implement healthy computing practices, ISPs' and Federal agencies' ongoing efforts to combat cyber threats can be rendered futile. For example, if users were

---

<sup>13</sup> GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, at 21-22 (July 2010) (“GAO Critical Infrastructure Report”), available at <http://www.gao.gov/new.items/d10628.pdf>.

<sup>14</sup> Verizon Business Risk Team, *2008 Data Breach Investigations Report* at 2-3 available at <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>.

more diligent in keeping their Microsoft Windows operating systems up-to-date, the Conficker worm would never have spread as significantly.<sup>15</sup>

The Commission could engage in a consumer education program to communicate to users a few simple steps—such as using antivirus software, diligently applying security patches, and operating only legally licensed applications and operating systems—that, if adopted, would make a dramatic difference in overall cyber security. The Commission should also consider participating in existing outreach campaigns. For example, the National Cyber Security Alliance (“NCSA”), of which AT&T is a partner, is a public-private partnership between the Department of Homeland Security and a broad cross-section of industry representatives including major hardware, software, defense, research and telecommunications companies. Through its website StaySafeOnline.org and its other efforts, NCSA strives to “educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals’ use, the networks they connect to, and our shared digital assets.”<sup>16</sup> The Commission could also coordinate with the NIST led National Initiative for Cybersecurity Education (“NICE”), which was created to establish a cyber security education program for the Nation.<sup>17</sup>

Indeed, numerous commenters in the Commission’s Cyber Security Certification Program proceeding agree that the Commission could play a valuable role informing users about cyber security issues. ATIS, for example, recommends that the Commission enhance

---

<sup>15</sup> See, e.g., See Mark Bowden, “The Enemy Within” *Atlantic Magazine* (June 2010) available at <http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098>.

<sup>16</sup> See National Cyber Security Alliance, “About Us – STAYSAFEONLINE.ORG” <http://www.staysafeonline.org/content/about-us> (last visited July 2, 2010).

<sup>17</sup> See National Initiative for Cybersecurity Education (NICE) Will Train Citizens To Use Computers Safely, available at <http://csrc.nist.gov/nice/index.htm>.

user education by, among other things, holding public workshops.<sup>18</sup> (ISC)<sup>2</sup> suggests that the Commission encourage the development of a K-12 educational programs and community college courses.<sup>19</sup> Sprint advocates a public awareness campaign that targets consumers and small businesses.<sup>20</sup> By pursuing these recommendations to engage consumers on cyber security issues directly and coordinating with the existing educational and awareness efforts like NCSA and NICE, the Commission can ensure that the public is receiving a clear, uniform and effective message.<sup>21</sup>

## **2. The Commission Should Advise and Assist Other Federal and International Cyber Security Initiatives.**

In addition to consumer education, as the expert agency on communications issues and the communications industry, the Commission could play a vital role by educating, advising and assisting other Federal and international governmental cyber security initiatives. As discussed more fully below, there is a multitude of different Federal agencies and public-private partnerships focused on cyber security issues. These various initiatives are often stove-piped in their application, but have cross-cutting purposes that create a confusing array of governmental programs in need of effective coordination. Although there are proposals for the White House, through the Executive Office of the President, to take the lead in

---

<sup>18</sup> ATIS Comments at 8.

<sup>19</sup> Comments of (ISC)<sup>2</sup>, PS Docket No. 10-93, at 6 (filed July 14, 2010).

<sup>20</sup> Comments of Sprint Nextel Corporation, PS Docket No. 10-93, at 12 (filed July 12, 2010).

<sup>21</sup> The Commission, on its own or in conjunction with other agencies, such as the Department of Commerce, could engage in a similar campaign with respect to operating system providers and application developers to raise awareness of the need to design cyber security protections into their products.

coordinating the various Federal cyber security efforts,<sup>22</sup> the Commission could still be of great assistance by providing its unique expertise and acting as a useful liaison with the communications industry.

The Commission has expertise on how commercial communications networks operate and on the market-based incentives for communications providers to safeguard their networks and customers that could enhance the government's implementation of existing cyber security programs. As such, the Commission should interact on an interagency basis with other governmental bodies to share its expertise and guide policies in an appropriate direction. As cyber threats are indisputably a global phenomenon, the Commission should also coordinate with the State Department on international cyber security outreach and education efforts for regulators and governments around the world.

**C. The Commission Should Not Impose Prescriptive Cyber Security Regulations on ISPs.**

Although the Notice does not indicate what actions the Commission may undertake as part of its cyber security roadmap, substantial practical and legal issues caution against imposing prescriptive regulation against ISPs.

**1. Regulating ISPs Would Weaken Rather than Strengthen Cyber Security.**

As the Notice properly recognizes, the first task for the Commission is to understand the nature of the cyber security it seeks to address. And, as AT&T and others have described in detail, ISPs are generally effective at both preventing cyber attacks and limiting the scope of those incidents when they occur. Thus, imposing prescriptive cyber security-oriented regulation or standards on ISPs would provide minimal benefits, if any, in protecting against

---

<sup>22</sup> See, e.g., H.R.4900 and S.3480. If enacted, these bills may vest substantial powers over interagency coordination, budgetary and procurement issues, and other matters to a cyberspace policy office within the Executive Office of the President.

cyber attacks. At the same time, however, regulating ISPs' cyber security efforts could seriously inhibit their ability to defend against cyber attacks.

Cyber security threats are a particularly insidious challenge to overcome not only because of the multi-level nature of the Internet ecosystem, but also because of their dynamic and constantly evolving nature. New versions of operating systems, applications and devices, and subsequently released software patches, are hacked as soon as, or even sometimes before, they become publicly available (i.e. "zero day attacks"). Veracode reports that "[i]n the past six months alone there have been multiple new zero-day vulnerabilities reported in Microsoft Windows."<sup>23</sup> Further, the sophistication and versatility of cyber attacks is increasing exponentially and requires rapid innovation and user vigilance to address.

In previous filings, AT&T has explained some of the key measures it uses to scrutinize traffic on its network and the capabilities it provides users to defend against malicious activities.<sup>24</sup> For example, AT&T monitors traffic patterns emanating from known origins of malicious activity as well as the overall traffic on its network. Complemented by proactive and reactive defensive techniques aimed at ensuring that the network is as secure as possible, these actions allow AT&T to automatically detect and mitigate attacks within the

---

<sup>23</sup> Veracode Press Release: Gartner Security & Risk Management Summit 2010, *Veracode State of Software Security Report Shows Suppliers of Cloud/Web-Based Applications Face Greatest Scrutiny by CXOs* (Sept. 22, 2010), available at C:\Documents and Settings\rv4902\Desktop\FCC Legal Work\Broadband Initiatives\Cybersecurity Proceedings\Veracode Press Release re Report (09.22.10).mht (last visited September 22, 2010). See also John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, Remarks at the Cyber Security Workshop at 17 (Sept. 30, 2009) transcript available at [http://www.broadband.gov/docs/ws\\_26\\_cyber\\_security.pdf](http://www.broadband.gov/docs/ws_26_cyber_security.pdf) (last visited September 22, 2010) (explaining that the number and speed of "zero day attacks" have dramatically increased).

<sup>24</sup> AT&T Certification Program Comments at 8-11.

network before they affect service to customers.<sup>25</sup> For business and government customers with enhanced security needs, AT&T's managed security services assess vulnerabilities, help provide network security, detect attacks, respond to suspicious activities, and provide for continuity of business operations in the event of an attack.<sup>26</sup> These enterprise security services include encryption, firewall protection, intrusion detection, authentication, and other services designed to prevent attacks, as well as remote backup and recovery solutions

AT&T is able to offer this wide range of security capabilities because, under the current "light touch" approach to regulation of IP-based services, it has wide latitude to invest in and deploy the security tools and practices that, based on expertise of its security specialists, AT&T believes are best suited to address today's cyber security threats. Based on AT&T's extensive experience managing a global IP network, innovation and flexibility are the greatest weapons against these varied, nefarious and adaptive threats.<sup>27</sup> Indeed, a provider's need for flexibility to respond to a wide range of possible cyber threats is analogous to a provider's need for wide latitude to take extraordinary measures following a major disaster. In those situations, the integrity and continued operation of the network is of paramount importance. In such emergency scenarios, the Commission often waives or suspends many of its rules to allow for quick, decisive action. For example, following Hurricanes Katrina and Rita, the Commission granted numerous applications for special temporary operating authority and waived many of its rules to provide regulatory relief to its

---

<sup>25</sup> *Id.* at 8-9.

<sup>26</sup> *See* AT&T NBP Public Notice # 8 Comments at 38-40.

<sup>27</sup> AT&T also refers the Commission to AT&T's comments filed in the Open Internet docket. Comments of AT&T Inc., GN Docket No. 09-191, WC Docket No. 07-52, at 75-78 (filed Jan. 14, 2009).

regulatees to facilitate quick restoration of networks and services to customers.<sup>28</sup> Combating cyber threats requires this same type of flexibility on a constant, year-round basis. Similarly, ISPs must be free from prescriptive regulation to retain the flexibility to respond to cyber security threats of all kind.

Any prescriptive regulations that limit an ISP's flexibility to innovate, no matter how well intentioned, would be a fundamentally static solution to a dynamic, constantly evolving problem. Indeed, whatever cyber security rules, guidelines or practices the Commission chose to adopt would be outdated before they were published in the C.F.R. Worse still, such government-mandated security practices could provide cyber criminals with a blueprint for improving their cyber attack capabilities. In particular, in the National Broadband Plan, the Commission recommended that the cyber security roadmap identify the most critical cyber security threats to the communications infrastructure and its end users and establish a two-year plan for the Commission to address these cyber threats.<sup>29</sup> If the Commission proceeds with the cyber security roadmap, the risks of divulging vulnerabilities or remedial measures counsels against providing significant details or specific guidance in the roadmap document or any related rules or guidelines. Hackers are notoriously efficient at exploiting vulnerabilities in software code and other systems. As noted above, new versions of software and devices and subsequently released software patches are hacked as soon as, or even

---

<sup>28</sup> See Written Statement of Kevin J. Martin, Chairman, Federal Communications Commission, Hearing on Public Safety Communications from 9/11 to Katrina: Critical Public Policy Lessons, Before the Subcommittee on Telecommunications and the Internet Committee on Energy and Commerce, United States House of Representatives, App. A (Sept. 29, 2005).

<sup>29</sup> Federal Communications Commission, *Connecting America: The National Broadband Plan*, Recommendation § 16.5, p. 321 (March 2010).

sometimes before, they become publicly available.<sup>30</sup> Publicizing specific network vulnerabilities in detail or the Commission's proposed efforts to address those vulnerabilities risks exposing information that is unknown to cyber criminals, or at best, not of current interest to them.<sup>31</sup> Any cyber security "roadmap" for the communications industry and other stakeholders must not also be a "roadmap" for cyber criminals; instead, it should merely emphasize the general areas of vulnerability and direct attention to areas to where improvements need to be made.

## **2. The Commission Should Coordinate with Other Federal Agency Cyber Security Efforts.**

Instead of approaching the issue of cyber security from a regulatory, Commission-centric perspective, the Commission should recognize the substantial work already in progress by other Federal agencies. Among the federal agencies involved in cyber security efforts are the White House Cyber Security Coordinator,<sup>32</sup> the Director of the Office of Management and Budget (OMB),<sup>33</sup> the Department of Homeland Security ("DHS"),<sup>34</sup>

---

<sup>30</sup> As John Nagengast, Executive Director, Strategic Initiatives for AT&T Government Solutions, explained at a recent Commission broadband workshop on cyber security, the number and speed of "zero day attacks" or incidents occurring on the day that a new security vulnerability is announced in the form of a software patch, have dramatically increased. John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, Remarks at the Cyber Security Workshop at 17 (Sept. 30, 2009) *transcript available at* [http://www.broadband.gov/docs/ws\\_26\\_cyber\\_security.pdf](http://www.broadband.gov/docs/ws_26_cyber_security.pdf) (last visited Nov. 9, 2009).

<sup>31</sup> *See* NCTA Comments at 5 ("Centralizing deliberations and standardized approaches regarding cyber security problems under the auspices of the Commission would not only impair effectiveness in dealing with security risks, it could also facilitate security breaches.").

<sup>32</sup> The Cyber Security Coordinator is responsible for setting a national agenda and for coordinating Executive Branch cyber security activities

<sup>33</sup> OMB is responsible for overseeing Federal agency information security policies and practices.

<sup>34</sup> DHS is the focal point for cyber security; provides consolidated intrusion detection, incident analysis and cyber response capabilities to protect Federal agencies' external access

DHS's U.S. Secret Service, DHS's Federal Bureau of Investigation, Department of Defense,<sup>35</sup> the National Science and Technology Council and its Committee on Technology ("NSTC"),<sup>36</sup> the Department of Commerce's National Institute of Standards and Technology (NIST),<sup>37</sup> and the Department of Commerce's National Telecommunications and Information Administration (NTIA).<sup>38</sup>

Each of these Federal agencies has its own programs to address cyber security, creating a complicated and often fragmented collection of Federal government initiatives to which ISPs and other private sector stakeholders must commit time and resources. As Melissa Hathaway, former Acting Senior Director for Cybersecurity at the National Security Council, pointed out "a recent cursory review identified more than 55 government initiated private-public partnerships in the area of cyber security."<sup>39</sup> These include the National Security Telecommunications Advisory Committee (NSTAC), U.S. Secret Service (USSS)

---

points, including access to the Internet, takes the lead in securing federal civilian systems, works with public and private stakeholders to protect critical infrastructure and key resources (CIKR)

<sup>35</sup> DOD is responsible for protecting military and national security systems

<sup>36</sup> NSTC serves as the coordinating organization over the Networking and Information Technology Research and Development (NITRD) program, which is the primary mechanism by which the U.S. Government coordinates its unclassified networking and IT research and development investments, including cyber security research and development

<sup>37</sup> NIST develops standards and guides for securing non-national security Federal information systems. It defines minimum security requirements for federally held information and for information systems.

<sup>38</sup> NTIA is the principal adviser to the President on telecommunications and information policies, works closely with other parts of government on broadband deployment, Internet policy development, securing the Internet namespace, and other issues.

<sup>39</sup> See Melissa Hathaway, "Why Successful Partnerships are Critical for Promotion Cybersecurity" [http://www.thenewnewinternet.com/2010/05/07/why-successful-partnerships-are-critical-for-promoting-cyber security/](http://www.thenewnewinternet.com/2010/05/07/why-successful-partnerships-are-critical-for-promoting-cyber-security/) (May 7, 2010).

Cyber Crimes Task Force, Federal Bureau of Investigation's InfraGard<sup>®</sup>, Computer Emergency Response Team/Coordination Center (CERT/CC), Communications Security, Reliability and Interoperability Council (CSRIC), formerly Network Reliability and Interoperability Council (NRIC), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Forum of Incident Response and Security Teams (FIRST), Communications - Information Sharing and Analysis Center (Communications-ISAC), ATIS - Network Reliability Steering Committee (NRSC), and National Cyber Security Alliance.

While AT&T fully supports the U.S. government's efforts to strengthen cyber security, this multitude of Federal programs and agency initiatives related to cyber security operating without sufficient coordination and organization creates inefficiencies and, at times, can be counterproductive. A U.S. Government Accountability Office ("GAO") report on the Comprehensive National Cybersecurity Initiative found that "[c]urrently, agencies have overlapping and uncoordinated responsibilities for cyber security activities that have not been clarified."<sup>40</sup> Another recent GAO report, citing cyber security experts, highlighted the need for a single or centralized government source for cyber-related information.<sup>41</sup> Given the extensive cyber security efforts already being undertaken by ISPs, and in light of the already crowded and at times uncoordinated government involvement in cyber security matters, adding another layer of complexity in the form of Commission regulations would be counterproductive.<sup>42</sup>

---

<sup>40</sup> GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative* at 2 (March 2010) available at <http://www.gao.gov/new.items/d10338.pdf>.

<sup>41</sup> GAO Critical Infrastructure Report at 15.

<sup>42</sup> See Comments of The National Cable & Telecommunications Association, PS Docket 10-93, p.4 (filed July 12, 2010) ("NCTA Comments") ("A centralized cyber security initiative

### **3. The Commission Has Not Yet Identified a Basis for Its Legal Authority over Cyber Security Issues.**

In all events, the Commission has not yet identified any specific legal authority to regulate the cyber security practices of ISPs and of other providers in the Internet ecosystem, particularly the software vendors whose products introduce significant cyber vulnerabilities into that ecosystem. As the D.C. Circuit's decision in *Comcast Corp. v. FCC* makes clear, it is incumbent upon the Commission to identify such authority before adopting any regulations in this area.<sup>43</sup> Moreover, for all of the reasons discussed above, adopting prescriptive regulations that limit the flexibility of ISPs to plan for and respond to cyber attacks, would undermine rather than advance the goal of improving cyber security.

### **III. CONCLUSION**

The record shows that the majority of cyber security vulnerabilities occur in the operating systems, application and end user layers of the Internet ecosystem. To effectively address these vulnerabilities, the Commission should participate in a comprehensive campaign, in coordination with other Federal agency efforts, such as NICE, to educate the relevant stakeholders about cyber security risks and measures that can be taken to mitigate those risks. At the same time, in light of the substantial efforts already undertaken by ISPs to combat cyber threats, the Commission should not adopt prescriptive regulatory requirements that limit ISPs' flexibility to respond to such threats.

---

that is coordinated and supervised by the Commission is not the optimal environment in which to ensure either of these necessary components.”).

<sup>43</sup> *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010).

Respectfully submitted,

**AT&T Inc.**

By: /s/ Robert Vitanza

Robert Vitanza  
Gary L. Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20th Street, N.W.  
Washington, DC 20036  
(202) 457-3076  
*Counsel for AT&T Inc.*

September 23, 2010