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

In the Matter of:	)	
Cyber Security Certification Program	)	PS Docket No. 10-93

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.

July 12, 2010

EXECUTIVE SUMMARY

AT&T Inc. ("AT&T") appreciates the opportunity to provide comments on the Federal Communications Commission's ("Commission") Notice of Inquiry and to share its perspective on the state of cyber security today. As the Internet becomes more essential to our way of life, cyber security will be increasingly indispensable.

Because of the interconnectedness of the Internet, cyber security requires an end-to-end approach that spans from the physical layer and the core IP network up through the application layer and device interface all the way to the users themselves. Today, a significant proportion of Internet vulnerabilities arise from the application and device layers, where even small security flaws are exploited by hackers to create vast networks of hijacked systems and to cause substantial economic and social damage. Technological vulnerabilities are compounded by the fact that many users do not take appropriate steps to protect themselves online, or fall victim to creative, socially engineered scams and attacks. Thus, to be effective, cyber security efforts cannot just focus on broadband Internet access service providers—as the Commission's proposed program would do—but must include operating system vendors, application developers, device manufacturers and the full spectrum of users. Further, in light of the varied, nefarious and adaptive nature of the threat, the greatest weapons in the cyber security fight are innovation and flexibility, and preserving these dynamics should be of paramount interest to the Commission.

The 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. In weighing the utility of a certification program, the Commission should recognize the wide-ranging cyber security efforts already underway, which are effectively promoted through market forces. For example, AT&T considers security to be a cornerstone of

the network management functions it performs in the United States and worldwide. AT&T has taken market-leading steps to educate and empower its customers through information and security tools tailored to the needs of those customers. In addition, there are numerous industry efforts, public-private partnerships, and federal programs currently underway that focus on enhancing cyber security. Rather than adding another layer of complexity, the Commission would more effectively contribute to cyber security by helping to coordinate and inform some of these existing programs.

Indeed, the Commission's certification proposal is premised on an incorrect assumption that there are insufficient market-based incentives for communications providers to implement effective cyber security practices. In fact, substantial incentives exist for communications providers to educate customers on cyber security policies and implement effective cyber security practices, and those providers will and do lose customers if they fail in that effort. Communications service providers, through substantial investment and innovation, have developed extremely sophisticated cyber security practices—all without the burden of prescriptive regulation. Users are sensitive to cyber security vulnerabilities; large business and government users, in particular, demand information about the cyber security practices of their communications service providers and adequate assurances that their sensitive data will be protected. The measures taken by communications service providers in response to these market pressures improve network security for all users. Moreover, the desire to avoid the significant economic and reputational damage that can be caused by a major cyber attack, coupled with intense competition among communications service providers, drives innovation in cyber security as service providers strive to constantly stay ahead of the curve.

While AT&T supports the Commission's focus on strengthening cyber security, the Commission's proposal for an ostensibly voluntary certification program for communications service providers raises substantial public policy, practical and legal questions that counsel against continuing to pursue the program. First, there is a real possibility that the proposed program could actually reduce the effectiveness of the industry's cyber security efforts. Complying with the program's fixed standards would limit the flexibility of communications service providers to manage their networks effectively in response to changing cyber threats as well as deter their incentive to innovate. Adopting public standards could also expose network vulnerabilities, potentially giving cyber criminals a roadmap to the security infrastructure and security vulnerabilities of participating networks. Moreover, the program could foster a false sense of security in Internet users who may have an exaggerated belief about the efficacy of network-based security techniques, particularly considering that operating system, application and device vendors would all be *excluded* from program coverage.

Second, beyond any potential security pitfalls that might result, it is not clear what practical value the program would add, whether it would be useful to network operators and whether they would even participate, especially in light of the significant logistical challenges faced. The Commission contemplates the creation or designation of several entities to manage the program, which likely would have to be funded, educated, updated, maintained and perhaps even staffed by industry members. Meanwhile, market forces and private agreements already provide many of the increased security benefits of a certification program. Thus, the program may not elicit significant participation by the industry or, worse, participation may come at the expense of diverting resources from other security activities that are potentially more effective. Additionally, the Commission has not articulated a clear statutory basis of legal authority to

adopt the certification program, nor does the voluntary nature of the proposed program obviate the need for such an articulation. As recent legal precedent makes clear, agencies can only act pursuant to Congressional authorization.

In lieu of the proposed certification program, AT&T suggests that the Commission consider options that would clearly be within its legal authority and focus on solutions for cyber security that draw from areas where the Commission has core strengths. These include consumer education, interagency coordination, and other important efforts that will have a clearer and more direct contribution to the fight against cyber security threats and crime. Moreover, the Commission has substantial expertise and relevant experience that could be contributed meaningfully to existing government programs and public-private initiatives. As such, the Commission should interact on both an interagency and an international basis with other governmental bodies to share its expertise and guide policies in an appropriate direction. AT&T believes such efforts will more effectively address cyber security than the certification program proposed.

TABLE OF CONTENTS

Page

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

In the Matter of:	)	
Cyber Security Certification Program	)	PS Docket No. 10-93

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") Notice of Inquiry ("NOI") pertaining to a proposal to create a "voluntary" cyber security certification program.[1] AT&T shares the Commission's concern regarding the serious economic and social harms posed by cyber security attacks, crimes and threats. AT&T also appreciates that, as the Internet becomes more essential to our way of life, cyber security will be increasingly indispensable to providing reliable and secure communications for all Americans.

Building effective defenses to cyber threats requires a multi-faceted approach to cyber security at all levels of the Internet ecosystem, including broadband service providers, operating system vendors, application developers, device manufacturers, and the full spectrum of users. Toward that end, the communication industry is addressing cyber security on multiple fronts—including through several established public-private partnerships. By these

[1] *See Cyber Security Certification Program*, PS Docket No. 10-93, *Notice of Inquiry*, 25 FCC Rcd 4345 (2010) ("NOI"). 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. *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").

efforts, the communications industry has achieved a remarkably successful record of preventing cyber security incidents and, when they do occur, of identifying them quickly and minimizing the damage. And, the communications industry has sufficient market-based incentives that continue to spur communications providers to proactively implement measures which adequately address cyber threats, protecting communications networks and the customers who use them and avoiding costs arising from cyber attacks.

Although AT&T supports the Commission's focus on strengthening cyber security, the Commission's certification proposal raises substantial legal, public policy and practical concerns. Rather than developing a new regulatory regime—which could, in practice, thwart Internet security and Internet security innovations—the Commission's cyber security efforts should instead draw from areas where the Commission has core strengths, such as in consumer education and interagency coordination. By focusing on its core competencies in this manner, the Commission's efforts can make a clear and immediate contribution to the fight against cyber security threats and cyber crime.[2]

I. CYBER SECURITY IS A COMPLEX ISSUE AFFECTING EVERY ASPECT OF THE INTERNET ECOSYSTEM FROM THE NETWORK LAYER TO THE APPLICATION LAYER.

As the Commission correctly observes in its NOI, "[i]n today's interconnected world, an increasingly greater amount of the nation's daily business depends on our rapidly growing broadband communications infrastructure."[3] Beyond their profound impact on business,

---

[2] It is important to note that cyber crime is, first and foremost, crime. Vulnerabilities in applications and networks are exploited by humans working alone, or increasingly, in criminal organizations. It is undeniably important to promote security at the end user, developer, and network operator levels. However, any approach to addressing this issue, including those discussed in this submission, must be coupled with effective law enforcement and crime prevention efforts.

[3] NOI at 4346, ¶ 2.

broadband communications have the potential to revolutionize nearly every aspect of our lives from education, health care, and energy efficiency to self-governance and cultural production. However, in order for the broadband infrastructure to fulfill this promise, it must be supported by secure communications platforms in which consumers, businesses, and governmental agencies can place their trust. This is a prerequisite to widespread adoption.

Cyber-based attacks pose serious economic and national security challenges. The White House, in its Cyberspace Policy Review, stated that a "growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure and government. These actors have the ability to compromise, steal, change or completely destroy information."[4] Consumer Reports recently estimated that cyber-based attacks have cost $8 billion over the past two years and affected over 1.2 million users.[5] There is no denying that cyber security is a serious issue and, given the complexity of the Internet environment, must be addressed throughout the private and public sectors through a multi-faceted approach.

For AT&T, cyber security is the collective set of capabilities, procedures, and practices that protect our customers and the services we provide to them from the full spectrum of cyber threats. Cyber security seeks to assure that the information, applications, and services our customers want are secure, accurate, reliable, and available wherever and

---

[4] "Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure," National Security Council, at 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last visited June 17, 2010).

[5] "Boom Time for Cybercrime: The economy and online social networks are the latest fodder for scams," Consumer Reports (June 2009), *available at* http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/overview/state-of-the-net-ov.htm (last visited Nov. 10, 2009).

whenever they are desired.[6] However, the network infrastructure is only one facet of the overall operational dynamic of the Internet, which also includes operating systems, applications, devices and human beings. To be effective, cyber security requires the efforts of entities at every layer of the interconnected and interdependent Internet ecosystem, including the individual consumer. Cyber security requires an end-to-end approach that spans from the physical layer and the core IP network up through the application layer and device interface all the way to the users themselves. Moreover, although the Commission has a role to play in this arena, it is only one among numerous government agencies, industry organizations, and public-private partnerships currently focused in whole or in part on addressing these issues.

Today, a significant proportion of Internet vulnerabilities arise from the application and device layers. In fact, IBM reports that World Wide Web ("Web") application vulnerabilities make up more than half of the disclosed vulnerabilities since 2006.[7] In particular, IBM points to the vulnerability of Web application plug-ins and document formats, indicating that "[t]hree of the five most prevalent malicious Web site exploits of 2009 were PDFs, one was a Flash exploit, and the other was an ActiveX control that allows a user to view an office document through Microsoft Internet Explorer."[8] The identification and resolution of such vulnerabilities is a continuing and ongoing process. Network operators may be challenged to cope with security vulnerabilities discovered in the operating systems of the routers running within the core IP networks; some companies hinder protection efforts by

---

6 *See* 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 (last visited Nov. 9, 2009) ("Nagengast Remarks").

7 IBM Security Solution, *X-Force 2009 Trend and Risk Report: Annual Review of 2009* at 5 (Feb. 2010) *available at* http://www-935.ibm.com/services/us/iss/xforce/trendreports/.

8 *Id.* at 6.

refusing to share sufficient information with network operators about known vulnerabilities in their programs until such information becomes public.

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. As a recent paper by the Internet Security Alliance ("ISA"), a multi-sector trade association focused on addressing issues of information security, framed 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."[9] The fact that such a large number of users fail to take this step greatly exacerbates a problem, discussed further below, caused by the regular and public release of security patches, which can expose critical vulnerabilities to hackers.[10]

Cyber criminals and hackers increasingly rely upon exploiting user carelessness, lack of sophistication or naïveté in ways that would be difficult or impossible to address at the network level. For instance, 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."[11] As Symantec explains, "more and more, attackers are going directly after the end

---

[9] Internet Security Alliance, *Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model* at 4 (2009).

[10] *See* Mark Bowden, "The Enemy Within" *Atlantic Magazine* (June 2010) *available at* http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098.

[11] *See* Kevin Haley, Symantec "Don't Read This Blog" http://www.symantec.com/connect/blogs/don-t-read-blog (Nov. 17, 2009).

user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent."[12] From the perspective of the attacker, targeting end users directly through social engineering is attractive because it can effectively bypass network and software security protections without the need for seeking to exploit any systemic technical vulnerabilities.

Even where all parties are acting responsibly, the challenges of cyber security are compounded by the dynamic and constantly evolving nature of cyber threats. New versions of software and devices and subsequently released software patches are hacked as soon as, or even sometimes before, they become publicly available.[13] Further, the sophistication and versatility of cyber attacks is increasing exponentially and requires rapid innovation and user vigilance to address. This is illustrated in the evolution of Conficker, a worm that emerged in 2008 and has created the largest network of infected computers (or "botnet") in the world, estimated to be in 7 million computers throughout 200 countries. Conficker has adapted quickly and has gone through several versions and upgrades. At various times, when the cyber security community identified a flaw in the worm, the worm was quickly updated before the flaw could be used to eradicate it.[14]

Although Conficker is among the most notorious of botnets because of its scope and sophistication, it has not, as of yet, manifested a clearly harmful agenda. Other malicious software has had much more invasive and damaging objectives. For example, a variety of

---

[12] *Id.*

[13] 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. *See* Nagengast Remarks at 17.

[14] *See* Bowden, *supra* note 10.

criminal organizations are believed to be operating small botnets based on Zeus or Zbot, which is actually a rentable toolkit available for a fee from the developer.[15] Once installed, the malware lays dormant on the victim's PC until the user logs-in to a financial institution to engage in online banking. Zeus then inserts itself into the middle of the transaction to capture the user's login credentials, forwarding them to the criminal element operating the botnet. Another harmful code, Koobface, was the first botnet to propagate through online social networking sites. Initially spreading over Facebook, Koobface has since adapted to infect users of numerous other sites including MySpace, Twitter, Friendster, Bebo, hi5, Tagged, Netlog, fubar and myYearbook.[16] Once a PC is infected with Koobface, it is instructed to download additional components that hijack browser searches, steal encryption keys, and act as a malicious webhost to capture new victims.

Innovation and flexibility are the greatest weapons against these varied, nefarious and adaptive cyber threats. As discussed further below, AT&T and others in the communications industry believe that prescriptive regulation, even an ostensibly voluntary certification program, would likely deter innovation, have little protective effect, and could actually undermine the cyber security efforts of the communications industry and existing public-private initiatives. In light of the ever-changing nature of cyber threats, network operators must retain the flexibility to react quickly and decisively when a vulnerability or attack is detected. Contrary to providing a helpful guide or a minimum set of best practices, regulatory

---

15 *See* Loucif Kharouni, "New ZBOT Variants Targeting European Banks" *TrendLabs Malware Blog*, http://blog.trendmicro.com/new-zbot-variants-targeting-european-banks/ (Mar. 23, 2010).

16 *See* Methusela Cebrian Ferrer, "The Allure of Social Networking" *CA Security Advisor Research Blog*, http://community.ca.com/blogs/securityadvisor/archive/2009/05/31/the-allure-of-social-networking.aspx (May 31, 2009).

cyber security standards could hamstring the network management efforts of communications service providers by preventing providers from modifying standard practices to suit particular cyber threats even if the modification might provide a more effective response.

II. CYBER SECURITY IS ACTIVELY ADDRESSED BY THE COMMUNICATIONS INDUSTRY IN A VARIETY OF WAYS.

The 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. For its part, AT&T takes a multifaceted approach to cyber security that is targeted at protecting its customers in the retail, enterprise and public sector markets. Further, numerous public-private initiatives regarding cyber security already exist and are actively supported by the communications industry. In weighing the utility of a certification program, the Commission should recognize these wide-ranging cyber security efforts already underway, which are effectively promoted through market forces and incentives as well as existing public and private sector initiatives.

A. AT&T Provides a Range of Cyber Security Solutions to All Its Customers.

For AT&T, cyber security is a 24 hour-a-day mission, and although it cannot stop every threat that targets its customers, AT&T considers security to be a cornerstone of the network management functions that it performs in the United States and worldwide. AT&T continually monitors traffic patterns on its network to identify malicious behavior and respond to vulnerabilities and attacks. This includes monitoring traffic patterns from known origins of malicious activity as well as tracking trends on the network ports themselves. This monitoring is complemented by an understanding of the realities of network usage. For example, network management techniques must be able to distinguish between normal spikes in traffic due to external events (such as increases in Short Message Service ("SMS") traffic

during American Idol), and malicious surges that could be produced by a Distributed Denial of Service ("DDoS") cyber attack.[17] This monitoring is complemented by proactive and reactive defensive techniques aimed at ensuring that the network is as secure as possible. The result is that AT&T possesses the capability automatically to detect and mitigate many attacks within its network infrastructure before they affect service to customers.

However, network management alone is not sufficient to protect against cyber threats, as it secures only one aspect of the entire Internet ecosystem. Absent further efforts, the insidious nature of cyber threats would allow attacks to occur at another level of the ecosystem, typically the user level. For its part, AT&T takes great efforts to educate users about the potential dangers of cyber threats and how to prevent and detect those threats. AT&T provides users with tools and information to assist them in securing their systems. AT&T provides a large body of security information on its webpage, including cyber security tips on abuse, antivirus and firewall protections, email security, parental controls and how to protect personal information.[18] AT&T also offers its users easy access to up-to-date security alerts, hosts security and support discussion forums moderated by AT&T experts, and offers the ability to chat with an AT&T service representative live online.

AT&T has taken steps to put proactive security tools into the hands of users. For example, AT&T makes its Internet Security Suite and SpamGuard available to all residential broadband Internet access customers—and for many customers these tools are provided free

---

[17] *See* Nagengast Remarks at 18-22. *See also* AT&T NBP # 8 Comments, at 34 (In a DDoS event, "[a]ttackers typically rent computer processing power, bandwidth, and storage online, which they then use to send a traffic overload to an online destination. This results in the destination becoming unavailable for its intended use.").

[18] *See, e.g.*, AT&T, "AT&T Safety Resources" http://www.att.com/gen/landing-pages?pid=6456; AT&T, "AT&T Support and Customer Service" http://www.att.com/esupport/.

of charge. These suites provide a full array of consumer antivirus, firewall, and spam protection applications, which help users guard against cyber threats and unwanted communications. Moreover, AT&T continues to explore new approaches to communicate with users about cyber security issues and empower them to be proactive in minimizing the damage that a cyber attack might produce. For example, AT&T works with users who are potentially affected by a "fast flux" and other types of malicious attacks.

With respect to its business users, as detailed in AT&T's comments responding to National Broadband Plan Public Notice # 8, AT&T offers a comprehensive package of managed security services under its suite of Security and Business Continuity Services, which assesses vulnerabilities, helps provide network security, detects attacks, responds to suspicious activities, and provides for non-stop operations.[19] These security services include encryption, firewall protection, intrusion detection, authentication, and other services designed to prevent attacks, as well as remote backup and recovery solutions that help ensure continuity of operations and a quick recovery when attacks do occur. To assist business users in understanding AT&T's comprehensive approach to security within its networks and throughout the AT&T enterprise, as well as maximizing the benefits of the various security solutions available to them, AT&T provides the AT&T Information & Network Security Customer Reference Guide, which contains an extensive description of AT&T's cyber security practices and is attached hereto at Appendix A.

AT&T's market-leading security services are also implemented in the government sector. Recently, AT&T Government Solutions became the first "Networx" contract holder to receive Authority to Operate ("ATO") from the General Services Administration ("GSA") for

[19] *See* AT&T NBP Public Notice # 8 Comments at 38-40.

implementation of Managed Trusted IP Services ("MTIPS").[20] The ATO enables AT&T to offer its cloud-based cyber security services to federal agencies across the entire United States Government. AT&T Government Solutions has already confirmed MTIPS task orders with the Federal Trade Commission and the Environmental Protection Agency.

B. Numerous Public-Private Partnerships Already Exist to Address Cyber Security Issues.

There is currently a wide array of public sector efforts and public-private partnerships underway focused on enhancing cyber security. 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 cybersecurity. Over 30 of these emerged out of the Department of Homeland Security ("DHS") alone."[21] AT&T participates in or coordinates with many partnerships with government entities, both within the United States and internationally. To list a few:

- National Security Telecommunications Advisory Committee (NSTAC)
- U.S. Secret Service (USSS) Cyber Crimes Task Force
- Federal Bureau of Investigation's InfraGard®
- Network Reliability and Interoperability Council (NRIC)
- Computer Emergency Response Team/Coordination Center (CERT/CC) – a global initiative
- Communications Security, Reliability and Interoperability Council (CSRIC)

---

[20] *See* Press Release, AT&T Inc., AT&T Is the First Networx Contract Holder to Receive Authority to Operate a Trusted Internet Connections (TIC) Compliant Service (June 2, 2010) *available at* http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=30856.

[21] *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-cybersecurity/ (May 7, 2010).

- Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) – a global initiative
- Forum of Incident Response and Security Teams (FIRST) – a global initiative
- Communications - Information Sharing and Analysis Center (Communications-ISAC)
- ATIS - Network Reliability Steering Committee (NRSC)
- National Cyber Security Alliance

AT&T fully supports the U.S. government's efforts to strengthen cyber security. However, the multitude of federal programs and agency initiatives related to cyber security can create inefficiencies and, at times, be counterproductive. A recent U.S. Government Accountability Office ("GAO") report on the Comprehensive National Cybersecurity Initiative found that "[c]urrently, agencies have overlapping and uncoordinated responsibilities for cybersecurity activities that have not been clarified."[22] Indeed, the President's NSTAC has an ongoing cyber security effort that overlaps some of the goals of the Commission's proposed certification program.[23] The sheer number of uncoordinated programs that attempt to address various aspects of cyber security presents the risk of diluting the impact of any one program. Moreover, communications providers, as well as users, would be better served by devoting their focus and limited resources to fewer, more coordinated programs. Rather than adding another layer, or multiple layers,[24] of complexity

---

[22] 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.

[23] *See* NCS, National Telecommunications Advisory Committee, http://www.ncs.gov/nstac/nstac.html; NSTAC, *Cybersecurity Collaboration Report* (May 21, 2009) *available at* http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf.

[24] The complexity and administration of the certification program envisioned by the NOI is demonstrated by the proposals in the NOI to utilize up to four entities, in addition to possible Commission oversight, for various tasks associated with the program—a body to

to the growing number of U.S. cyber security government initiatives, AT&T respectfully suggests that the Commission—as the expert agency on the communications industry—help coordinate and inform existing programs in order to improve their effectiveness, while decreasing the burdens of participation for communications service providers.

C. Market Incentives Drive Innovation in Cyber Security.

The proposed certification program arises from incorrect conclusions in the NOI — that large business users are not educated about communications providers' cyber security practices, that users will not switch communications providers based upon cyber security factors, and that there are insufficient market-based incentives for communications providers to implement effective cyber security practices.

> We believe that large organizations and commercial entities in particular are interested in the cyber security practices of their communications service providers, but note that these customers of communications services have no effective way of knowing what the cyber security practices of competing providers may be. The lack of such information likely removes at least one significant incentive for providers fully to implement the NRIC best practices, in that they do not risk losing customers to networks with better security practices. The reduced incentive for heightened cyber security likely is compounded because a particular provider may not be motivated to exceed the security level of other interconnected network operators.[25]

In fact, substantial incentives exist for communications providers to continually improve their cyber security practices, as many large business and government customers are educated on cyber security policies and providers will and do lose those customers if cyber attacks against their networks are successful.

---

determine the providers to be certified, NOI, at 4355-56, ¶¶ 34-38, a body to determine how auditors can be accredited, NOI, at 4356, ¶40, a body to advise auditors how to assess a provider's cybersecurity efforts, NOI, at 4358, ¶¶44-45, and a body to create and operate a public database with cyber security information, NOI, at 4358-59, ¶ 48.

[25] NOI at 4348, ¶ 7.

Communications service providers, through substantial investment and innovation, have developed extremely sophisticated cyber security practices—all without the burden of prescriptive regulation. These cyber security practices developed because the communications industry understands that those service providers which operate the most reliable and secure networks stand to gain the most in an open marketplace. Compromised networks are inherently unreliable and produce a lack of user trust in the network, which inevitably leads these users to reject the providers' services. This dynamic provides substantial economic incentive for communications service providers to continually build greater protections into their platform for the users that rely on it.

Contrary to the unsupported conclusions in the NOI, users are sensitive to cyber security vulnerabilities. Large business and government users, in particular, demand information about the cyber security practices of their communications service providers and adequate assurances that their sensitive data will be protected. To meet the demand for information related to its cyber security practices, AT&T developed and distributes to business and government users the AT&T Information & Network Security Customer Reference Guide, which is attached hereto as Attachment A.[26] These business and government users also often demand contractual commitments that their information is secure. The Federal Government itself seeks these assurances by requiring communications service providers to obtain authority from the GSA to offer their MTIPS to federal agencies. Improvements to networks and cyber security practices that communications providers make in response to these market incentives also benefit individual consumers.

[26] The Commission must be mindful that, while communications providers may provide users with information about cyber security measures the providers take to protect user information, providers should keep certain security information out of the public sphere and thus out of the hands of potential cyber criminals.

Even the prospect of a cyber attack that adversely affects individual consumers provides substantial incentives for providers to protect their networks. Successful cyber attacks produce a myriad of damages to communications service providers. Cyber attacks may cause service outages or the disclosure of confidential consumer information, either of which could cause consumers to switch service providers.[27] In addition to foregone revenue from lost customers, communications service providers also incur significant monetary costs to notify customers of an illicit disclosure.[28] Further, cyber attacks may lead to costly litigation, regulatory investigations, contract disputes, and reputation damage.[29]

AT&T is not the only provider driven to ensure cyber security protection and innovation. It faces significant competition in the managed security services market from numerous other entities, including IBM, British Telecom, Orange, Symantec, T-Systems, Tata Communications, Verizon and Telefonica Multinational Solutions. For example, although AT&T received the first GSA authority to offer its MTIPS to federal agencies,[30] other major

---

[27] Bruce S. Schaeffer, Henfree Chan, Henry Chan and Susan Ogulnick, "Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others," Wolters Kluwer Law & Business, *available at* http://business.cch.com/franlaw/cybercrime_whitepaper.pdf (last visited Nov. 10, 2009) ("*Cyber Crime White Paper*").

[28] *Cyber Crime White Paper* at 4.

[29] *Cyber Crime White Paper* at 3. *See also* "Data and Contacts Vanish From Sidekick Phones," Los Angeles Times (Oct. 12, 2009), *available at* http://www.latimes.com/business/la-fi-sidekick13-2009oct13,0,3031857.story (last visited Nov. 10, 2009) (describing a recent service disruption to T-Mobile's Sidekick phone that caused some subscribers to cancel contracts); Ina Fried, "Lawsuits Filed Over Sidekick Outage," CNET News (Oct. 14, 2009), *available at* http://news.cnet.com/8301-13860_3-10375240-56.html (last visited Nov. 10, 2009) (describing lawsuits filed against T-Mobile and Microsoft relating to data loss caused by a service outage to the Sidekick phone); "AT&T E-mail Apologizes for iPad Data Breach, cnet news (June 13, 2010), *available at* http://news.cnet.com/8301-1009_3-20007564-83.html (last visited July 5, 2010).

[30] *See* Press Release, *supra* note 19.

industry players, such as Qwest, Sprint and Verizon, have also received awards from DHS to be MTIPS providers.[31] The fierce competition in this area drives innovation and efficiency, as communications service providers must constantly strive to deliver the best security services to their customers as quickly as possible.

These market forces belie the conclusions in the NOI that form the foundation for the certification program and clearly demonstrate that there are ample incentives for communications providers to invest in cyber security measures. These market forces spur innovation in cyber security and offer the best prospect that communications service providers will continue to provide safe and reliable service to users. The Commission's proposed certification program will likely provide no greater incentive to enhance cyber security than those market-based incentives that already exist. Instead, as discussed more fully below, it will more likely do just the opposite.

III. THE PROPOSED CERTIFICATION PROGRAM RAISES SIGNIFICANT PUBLIC POLICY, PRACTICAL AND LEGAL CONCERNS.

The Commission's proposal for an ostensibly voluntary certification program for communications service providers raises substantial public policy, practical and legal questions that counsel against continuing to pursue the program. As an initial matter, AT&T questions whether the goal of strengthening cyber security will be achieved with the certification program in light of its questionable efficacy and some significant practical challenges posed by its implementation. Moreover, the Commission has not articulated a clear statutory basis of legal authority to adopt the certification program, nor does the description of the proposed program as "voluntary" obviate the need for such an articulation.

---

[31] *See* Jason Miller, "GSA, DHS Approve First Governmentwide Cyber Provider" *Federal News Radio* (June 7, 2010) *available at* http://www.federalnewsradio.com/?sid=1971233&nid=35.

A. The Commission's Proposed Certification Program Raises Public Policy Concerns.

There are significant public policy and practical reasons to believe that the Commission should not adopt the proposed certification program. Indeed, there is a real possibility that the proposed program would actually reduce the effectiveness of industry's cyber security efforts. The proposal, whether intended or not, would result in a static program to address a dynamic problem. Complying with the program's fixed standards, even if broadly drafted and applied, would limit the flexibility of communications service providers to respond effectively to changing cyber threats through intelligent network management as well as deter their incentive to innovate. Moreover, the standards set by the program could establish a "least common denominator" of security measures that any industry member could satisfy and which would be practically meaningless. Adopting public standards could also expose network vulnerabilities, providing a map for cyber criminals. And, the resources necessary to develop, apply to and comply with the program would distract providers from participating in more effective government programs and public-private cyber security efforts.

Even if these harms are avoided, it is not clear whether any marginal cyber security gains resulting from the program would justify the significant logistical challenges involved in its adoption. In a recent paper on cyber security strategy, ISA directly addressed the low likelihood of success of a government-mandated cyber security program. As ISA points out "[a] system of regulatory mandates applied to the broad and diverse private sector is unlikely to be effective in generating . . . substantial improvements in private sector cyber security. In fact, such a system would almost certainly be counter-productive, from both a national economic, as well as a national cyber security perspective."[32]

[32] Internet Security Alliance, *supra* note 9, at 2.

The program envisioned in the NOI would likely reduce the flexibility of communications service providers and slow down their responses to cyber threats due to the restraints that the program would implement over time and concerns about how aggressive protection actions could be interpreted by the program's auditors. Placing a government-sponsored seal of approval on certain technology and business practices will tend to counteract existing incentives to be dynamic and innovative. Because "[t]he process of developing effective regulations is inherently time consuming," ISA explains, "there is unanimous agreement that any regulations specific enough to assure improved cyber security would become outdated soon after their enactment."[33] Thus, auditors likely will be constantly reviewing against standards that, at best, are outdated and, at worst, interfere with effective response efforts.

Even more damaging than simply slowing down private sector response times, the creation of the certification program could create perverse incentives to remain static rather than to innovate. For instance, once a company has received program certification, it will likely rely on its certification and be less likely to continue updating its technology or experimenting with new approaches to cyber security. A company may feel foreclosed from innovating in a way that may better meet a new threat if doing so risks rendering them non-compliant with the program's standards. User expectations would also be affected, as cyber security demands and assurances sought by large business customers, which can drive innovation and creative cyber security measures, risk being replaced by assurances that the provider has received Commission certification, regardless of whether the certification

[33] *Id.*

encompasses the protections that are best suited to that customer.[34] Worse, the more widely recognized the program is by users, the stronger this anti-innovation incentive will grow as program certification would surpass the market benefits of providing truly dynamic and responsive cyber security.

On a related note, the program could instill a false sense of security in some users. Even for subscribers of the most diligently and proactively secured networks, greater risks lie in the applications, device and user layers. However, as the proposed certification would apply only to "communications service providers," these vulnerabilities would likely not be addressed by the program. A profound risk exists that users might assume that since the Federal government is addressing the issue, they are fully protected. Many users will not understand this distinction and will expect that by subscribing to a certified communications service provider, they have done all that is necessary to protect themselves from cyber threats, causing them to fail to take other necessary steps or to ignore the signs of cyber attacks when they do occur.

There are additional causes for concern regarding unintended consequences of adopting the certification program. For example, by publicizing the network security practices of communications service providers, the program also runs the risk of exposing network vulnerabilities. As discussed above,[35] hackers are notoriously efficient when it comes to exploiting vulnerabilities in software code and other systems. The certification

---

[34] The NOI fails to address how to resolve the situation where existing contractual commitments between communications service providers and large businesses to implement cyber security initiatives, which may be tailored to the needs of the business, conflict with the requirements of the certification program.

[35] *See supra* pp. 4-8.

program risks making their tasks even easier by potentially providing a roadmap to the security infrastructure and security vulnerabilities of participating networks.

These weaknesses are all amplified by the fact that, to the extent that the program attracts widespread industry or public attention, the proposed certification program may distract from more effective government programs and public-private partnerships that are ongoing elsewhere. As discussed above, there are currently numerous cyber security initiatives within the federal government that rely in part upon participation by the private sector. In many cases, these initiatives have already implemented or are in the process of designing best practices, standards and techniques for cyber threat monitoring, prevention and response. However, unlike some other programs, the Commission intends for the certification program to be highly visible to the public and to influence consumer decision-making in the communications marketplace. Regardless of its actual efficacy, if the Commission implements and is successful in attracting significant attention to the proposed certification program, it may become a competitive necessity to participate in it, even at the expense of withdrawing resources from other, potentially more effective initiatives before those other efforts have the opportunity to realize their full potential.

B. The Commission's Proposed Certification Program Is Unlikely to Offer Additional Protection for Consumers or to Elicit Broad Industry Participation.

Beyond any potential security pitfalls that might result, it is not clear what practical value the proposed certification program would add, whether it would be useful to communications service providers and whether they would even adopt it, especially in light of the significant logistical challenges faced. For example, the Commission proposes the undertaking of substantial new standards-setting, monitoring and review burdens. To successfully implement the program, the Commission would need to oversee the development

and updating of security standards; the recruitment, training and management of auditors; and the crafting, monitoring and enforcement of program rules. Even the agency itself acknowledges in the NOI that "we do not believe that the Commission has the substantial resources needed to participate in the daily operation of the proposed cyber security certification program."[36]

Ultimately, the Commission contemplates the creation or designation of up to four entities to manage the program in addition to possible Commission oversight—an entity to determine the providers to be certified,[37] an entity for the accreditation of auditors,[38] an entity to advise auditors on assessing a provider's cyber security efforts,[39] and an entity to create and operate a public database with cyber security information.[40] Each of these entities likely would have to be funded, educated, updated, maintained and perhaps even staffed by industry members. Given the agility and resourcefulness of cyber attackers, industry security efforts have to be highly fluid and focused on remaining responsive. As noted above, it is unlikely that any government program, and especially a program with multiple third party entities, even if cooperatively managed, will be able to adjust its standards and educate auditors rapidly enough to keep pace with sophisticated cyber threats or the need of the communications industry to keep pace identifying and defending those threats. Resources spent attending to the management and operation of the certification program would be resources diverted from other, more effective cyber security efforts.

---

36 NOI at 4352, ¶ 23.

37 *Id.* at 4355-56, ¶¶ 36-38.

38 *Id.* at 4356, ¶ 40.

39 *Id.* at 4358, ¶¶ 44-45.

40 *Id.* at 4358-59, ¶ 48.

Market forces and private agreements already provide many of the increased security benefits of a certification program. For example, in additional to contractual cyber security commitments, many communications service providers are already subject to audits of security practices on behalf of large business users, particularly those in the financial, health and utility sectors. These market-driven contractual obligations are a prerequisite to serving those business users and result in improving overall security for all users. Furthermore, some services are already certified by certain organizations for special purposes or where regulatory and statutory provisions require heightened industry-specific protections.[41]

To illustrate, in AT&T's case, external audits and certifications are performed for specific services where business requirements merit third party attestations or compliance evaluation, such as SAS 70, SysTrust and Payment Card Industry (PCI) Data Security Standard (DSS). Moreover, AT&T offers its business customers services to assist their compliance with existing regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and security standards as defined through governing bodies such as the European Union. Against this backdrop, the Commission's proposed certification program would seem only to add one more layer of expense and effort, with little to no concomitant gain in actual security.

Finally, it is not clear that the program would elicit significant industry participation. Communications service providers would assess the value of the program based upon a number of factors, such as: (i) user perception about the value and visibility of the certification; (ii) the ultimate obligations and requirements associated with the program; (iii) the burdens of compliance, including the need to share proprietary security information with

[41] *See, e.g.*, Attachment A at 11-12 (discussing "Internal and External Reviews and Audits").

outside auditors, competitors and perhaps the wider public; and (iv) the utility of the certification to offer meaningful protection to users in light of users' inevitable interaction with content, application and service providers that present substantial cyber security vulnerabilities.

This analysis may lead many communications service providers to conclude that participation not only is overly burdensome, but also may create additional vulnerabilities and risks to their operations. Because of the interconnectedness of online interactions, anything less than near ubiquity will result in largely meaningless gains in cyber security protection. The likely result in such a situation would be the expenditure of significant resources by the Commission and by industry with little measureable return.

C. The Commission's Legal Authority to Establish the Proposed Voluntary Certification Program Is Unclear.

Putting aside the policy and practical weaknesses of the certification program, the Commission has not identified any compelling basis for statutory jurisdiction under Title I, Title II or any other provision of the Communications Act that would allow it to establish a cyber security certification program, as it is required to do with any regulatory action. Especially in light of the D.C. Circuit's recent decision in *Comcast Corp. v. FCC*,[42] it is incumbent upon the Commission to clearly identify a statutory basis for its action before it attempts to take new regulatory measures over broadband Internet access services. The Commission's jurisdiction over the application and device layers—which contain the majority of vulnerabilities exploited by viruses, Trojans and worms—seems particularly unclear, as many of the entities involved in developing these products are not otherwise regulated by the Commission. Where it is not clear that there is an explicit statutory grant of authority, the

[42] *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010).

appropriate solution is for the Commission to look to Congress for a clarification of its jurisdiction.

The ostensibly voluntary nature of the proposed certification program would not cure any possible jurisdictional defects. An agency's authority does not expand solely because the program it enacts is voluntary.[43] It follows, then, that where an agency has not been conferred power to act, it cannot act—regardless of whether it seeks to mandate or to encourage compliance with the particular program. Absent a statute conferring authority to enact the certification program, the Commission does not have authority to do so, whether it is voluntary or mandatory.[44] In the past, Congress has specifically delegated authority to create voluntary programs, such as the Energy Star program, at the agency level.[45] Thus, Congress is aware of its obligation to delegate authority to agencies, even where the goal is voluntary

---

[43] A "federal agency [is] a creature of statute" that has "no constitutional or common law existence or authority" other than "those authorities conferred upon it by Congress." *Michigan v. EPA*, 268 F.3d 1075, 1081 (D.C. Cir. 2001). Accordingly, "'administrative agencies may [act] only pursuant to authority delegated to them by Congress.'" *Comcast*, 600 F.3d at 654 (quoting *Am. Library Ass'n*, 406 F.3d at 691). "[I]f there is no statute conferring authority, a federal agency has none." *Michigan*, 268 F.3d at 1081; *see also North Carolina v. E.P.A.*, 531 F.3d 896, 922 (D.C. Cir. 2008) (same). "[A]n agency literally has no power to act . . . unless and until Congress confers power upon it." *Louisiana Public Service Comm'n v. FCC*, 476 U.S. 355, 374 (1986).

[44] *Cf. Ethyl Corp. v. EPA*, 51 F.3d 1053, 1060 (D.C. Cir. 1995) ("Were courts to presume a delegation of power absent an express withholding of such power, agencies would enjoy virtually limitless hegemony, a result plainly out of keeping with Chevron and quite likely with the Constitution as well.").

[45] *See* 42 U.S.C. § 6294a(a) ("There is established within the Department of Energy and the Environmental Protection Agency a voluntary program to identify and promote energy-efficient products and buildings in order to reduce energy consumption, improve energy security, and reduce pollution through voluntary labeling of, or other forms of communication about, products and buildings that meet the highest energy conservation standards."); *see also*, 7 U.S.C. § 4607(c)(1) (". . . the Honey Board, with the approval of the Secretary, may establish and carry out a voluntary quality assurance program concerning purity standards for honey and honey products."); 7 U.S.C. § 8102(b)(1) ("The Secretary, in consultation with the Administrator, shall establish a voluntary program under which the Secretary authorizes producers of biobased products to use the label 'USDA Certified Biobased Product'").

compliance. In the instant case, it is unclear from where statutory authority to enact the proposed program will derive.

Moreover, the voluntariness of the certification program may turn out to be illusory and coercive. Even if a network operator were to choose not to participate, the program could become a *de facto* industry standard and compliance may become a measure of "reasonableness" such that non-participants would expose themselves to potential legal liability or Commission scrutiny. The Commission should not be in a position to coerce, under the auspices of "voluntariness," compliance with prescriptive industry regulations that it would be unable to enact as a lawful mandate. Before proceeding any further, the Commission should clearly articulate a valid statutory framework conferring authority to create the contemplated program.

IV. THE COMMISSION CAN ADVANCE CYBER SECURITY PROTECTIONS THROUGH MORE EFFECTIVE STEPS.

In lieu of the proposed certification program, the Commission should consider undertaking actions that are clearly within its legal authority and more likely to have an immediate beneficial impact on the provision of cyber security protections. First, the Commission could participate in a strategic consumer education campaign with the goal of directly impacting one of the key struggles in cyber security—the low rate of user adoption of proven protection mechanisms. Secondly, rather than create a new, administratively burdensome and suspect cyber security initiative, the Commission should take advantage of its internal expertise and understanding of key communications industry issues by coordinating with other ongoing public sector cyber security programs.

A. The Commission Should Educate Consumers Regarding Responsible Cyber Security Practices.

Rather than regulating a communications industry that is already effectively addressing the challenges of cyber security threats, the Commission could 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 often 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 breeches were considered avoidable through the use of reasonable controls.[46]

In fact, the tools for users to protect themselves are widely available, but they need to be used and kept up to date to be effective. Unless users develop and implement healthy computing practices, the efforts already being taken by the communications industry can be rendered futile. For example, if users were more diligent in keeping their Microsoft Windows operating systems up-to-date, the Conficker worm would never have spread as significantly.[47]

AT&T and other communications service providers work with a variety of external organizations to promote online safety education and awareness.[48] To augment those industry efforts, the Commission could also 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

---

[46] Verizon Business Risk Team, *2008 Data Breach Investigations Report* at 2-3 *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[47] *See, e.g.*, Bowden, *supra* note 10.

[48] *See, e.g.*, AT&T NBP # 8 Comments, at 40-41.

adopted, would make a dramatic difference in overall cyber security. The Commission demonstrated the success of its consumer outreach capabilities in the lead-up to the digital television transition, wherein the Commission implemented a coordinated and strategic educational campaign that succeeded in delivering key bits of essential information to millions of Americans. Additionally, during the National Broadband Plan and other recent proceedings, the Commission demonstrated an ability to attract significant consumer attention via its website and online social networking activities. The Commission could take advantage of this attention by maintaining on its notification platform useful information, links, and free tools for consumers to ensure their devices are secure.

Although the Commission clearly has the ability and skill set required to undertake a significant consumer education effort, to expedite the benefits of such an effort the Commission should 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."[49] By coordinating with an existing effort like NCSA, the Commission can ensure that the public is receiving a clear, uniform and effective message.

[49] *See* National Cyber Security Alliance, "About Us – STAYSAFEONLINE.ORG" http://www.staysafeonline.org/content/about-us (last visited July 2, 2010).

B. 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 above, 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 something of a morass of governmental programs that demand effective coordination. Although there appears to be a consensus developing in Congress that the White House, through the Executive Office of the President, will take the lead in coordinating the various Federal cyber security efforts,[50] the Commission could still be of great assistance by providing its unique expertise and acting as a useful liaison with industry.

The Commission has crucial expertise on how commercial communications networks operate and on the incentives inherent in the market for communications services that could benefit 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.

---

[50] *See, e.g.*, H.R.4900 and S.3480. Depending on whether any final action is take and the form that it takes, these bills could give substantial powers over interagency coordination, budgetary and procurement issues, and other matters to a cyberspace policy office within the Executive Office of the President.

Beyond the measures suggested above, the Commission should continue to explore opportunities to have a positive impact on cyber security in ways that are sensible, efficient and within its legal authority. However, the Commission should remain mindful of applying regulatory regimes, such as renewed common carrier obligations or restrictive network management rules, that could hinder the ability of broadband Internet access service providers to effectively protect their networks and would ultimately chill development in cyber security. At all times, the Commission should ensure that its regulations preserve and enhance the flexibility of the private sector to invest and innovate to defend against the constantly changing threats to the Internet ecosystem.

V. CONCLUSION

AT&T reiterates its support for the goals of promoting security on the Internet. In order for America to enjoy the unparalleled benefits of broadband technologies, it must have a safe communications platform that inspires the confidence that consumers and businesses demand. Contrary to the unsupported conclusions in the NOI, substantial market-based incentives exist for communications service providers to implement effective network protection measures, as evidenced by the sophisticated cyber security practices currently in place. Although work remains to be done to address cyber security throughout the Internet ecosystem, a Commission-run certification program for communications service providers would offer no greater incentives for innovation and diligence in cyber security than those already provided in the market. Moreover, the Commission's proposed program stands a significant chance of harming existing cyber security efforts. Rather than proceed with the proposed certification program, the Commission should instead position itself as a major player in effectively promoting cyber security by leading the effort to improve customer education and intergovernmental coordination.

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.

July 12, 2010

ATTACHMENT A:

AT&T INFORMATION & NETWORK SECURITY CUSTOMER REFERENCE GUIDE

Your submission has been accepted

ECFS Filing Receipt - Confirmation number: 2010712350759

Proceeding

Name	Subject
10-93	In the Matter of Cyber Security Certification Program.

Contact Info

Name of Filer: AT&T Services, Inc.
Email Address: th5467@att.com
Attorney/Author Name: AT&T Inc.

Address

Address For: Filer
Address Line 1: 1120 20th Street, NW
Address Line 2: Suite 1000
City: Silver Spring
State: MARYLAND
Zip: 20036

Details

Type of Filing: COMMENT

Document(s)

File Name	Custom Description	Size
AT&T Cybersecurity NOI Comments final.pdf		155 KB

Disclaimer

This confirmation verifies that ECFS has received and accepted your filing. However, your filing will be rejected by ECFS if it contains macros, passwords, redlining, read-only formatting, a virus, or automated links to other documents.
Filings are generally processed and made available for online viewing within one business day of receipt. You may use the link below to check on the status of your filing:
http://fjallfoss.fcc.gov/ecfs/comment/confirm?confirmation=2010712350759
For any problems please contact the Help Desk at 202-418-0193.