Before the
Department of Commerce

In the Matter of	**)**	
	)	
Cybersecurity, Innovation and the Internet Economy	**)**	**Docket No.: 110527305–1303–02**
	)	
	)	

COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION

Robert Mayer
Kevin G. Rupy
Paul Eisler
United States Telecom Association
607 14th Street, N.W.
Suite 400
Washington, D.C. 20005
(202) 326-7200

August 1, 2011

TABLE OF CONTENTS

* * *

Before the
Department of Commerce

In the Matter of)
)
Cybersecurity, Innovation and the Internet Economy) **Docket No.: 110527305–1303–02**
)
)

COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION

I. INTRODUCTION

The United States Telecom Association (USTelecom)[1] is pleased to comment on the Notice and Request for Public Comments (*Notice*)[2] issued by the Department of Commerce (Department) regarding its green paper titled, "Cybersecurity, Innovation and the Internet Economy."[3] USTelecom appreciates the Department's sense of urgency regarding cybersecurity and shares the Department's goal of limiting malicious Internet activity, as such activity undermines the security interests of users and businesses.

The Department's green paper proposes the establishment of an Internet and Information Innovation Sector (I3S), which would work in partnership with the Department to develop best practices that may eventually become industry standards. The Green Paper correctly

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] Notice and Request for Public Comments, *Cybersecurity, Innovation, and the Internet Economy*, 76 Fed. Reg. 115 (June 15, 2011) (*available at* http://www.ntia.doc.gov/frnotices/2011/FR_cybersecurity_06152011.pdf) (visited July 27, 2011) (*Notice*).

[3] Department of Commerce, *Cybersecurity, Innovation and the Internet Economy* (*available at* http://www.ntia.doc.gov/internetpolicytaskforce) (visited July 27, 2011) (*Green Paper*).

acknowledges that the difficulties associated with securing cyberspace are often shared among a wide array of stakeholders in the evolving Internet ecosystem. The green paper also recognizes that industry members are engaged in multiple ongoing discussions, as well as partnerships, with other government entities, including the Department of Homeland Security (DHS) and the Department of Defense (DOD). If the Department decides to move forward with defining a new sector, USTelecom recommends that the Department focus its efforts on functions and services that will have the largest impact on enhancing cybersecurity, rather than defining a new sector that is based simply on a particular type of technology. USTelecom's recommended approach will help avoid duplication of efforts and market distortions, while also ensuring that valuable government and private sector resources are not wasted.

When industry members gain a clear understanding of what the proposed partnership with the Department entails, they will be better able to leverage the partnership's advantages to enhance their cybersecurity efforts. The Department could further promote these efforts by incentivizing voluntary investment, information-sharing, and best practices, as well as by working with industry to advance cybersecurity education and research.

II. ANY DEFINITION OF "I3S" SHOULD ACKNOWLEDGE THE BROAD NATURE OF THE INTERNET ECOSYSTEM.

In its Notice, the Department asks how "I3S" should be defined and what kinds of entities should be included.[4] Rather than base the definition of this sector on any type of technology, USTelecom maintains that any discussion of cybersecurity must address all aspects of the Internet environment, to include products, functions and services, such as software developers, device manufacturers and network service providers. Such a holistic approach is essential, based on the complex environment that comprises the Internet.

[4] *Notice*, p. 34966.

The Internet is a highly complex global system of networks, the product of connections that allow for interaction between indeterminable millions of individual systems each day. Though these structures differ in terms of size, capacity, function, and purpose, together they form an expansive and dynamic ecosystem through which massive amounts of data are transferred and exchanged. In this sense, the Internet has developed an organic quality insofar as it continually grows and adapts in response to newly added systems, functions and services.

For example, a recent study from Cisco concluded that in 2008 the number of devices connected to the Internet exceeded the number of people on earth – and by 2020, Cisco projects there will be 50 billion devices connected to the Internet.[5] Similarly, while concepts such as cloud computing were viewed as a "risky bet" a mere five years ago,[6] Amazon recently announced that its Simple Storage Service holds more than 449 billion objects and processes up to 290,000 requests per second for them at peak times.[7] As such, any definition the Department adopts pertaining to cybersecurity must acknowledge the broad and diverse nature of products, services and devices that comprise the Internet.

Defining the Department's cybersecurity efforts in such a manner ensures that any accompanying policy initiatives flow throughout the Internet ecosystem. This is particularly important, since actors operate in both an autonomous and interdependent fashion. As a result, changes in one service may implicate the entire network, and by extension the Internet

[5] Arik Hesseldahl, *Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting*, All Things Digital website, July 14, 2011 (available at: http://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-internet-is-and-how-big-its-getting/?mod=googlenews) (visited July 27, 2011).

[6] Bloomberg Business Week, *Jeff Bazos' Risky Bet*, November 13, 2006 (available at: http://www.businessweek.com/magazine/content/06_46/b4009001.htm) (visited July 28, 2011).

[7] Amazon Web Services Blog, *Amazon S3 – More Than 449 Billion Objects*, July 19, 2011 (available at: http://aws.typepad.com/aws/2011/07/amazon-s3-more-than-449-billion-objects.html) (visited July 28, 2011).

ecosystem itself. Consequently, it is impossible to isolate individual components of the Internet ecosystem, since regulating some components (*e.g.*, broadband networks) would in no way guarantee the security in other equally important components (*e.g.*, software products).

For example, the recent attack on Google and at least thirty-three other companies from an entity in mainland China exemplifies how various Internet components are inextricably linked.[8] The theft of Google's information, including a password system that controlled millions of users' access to a variety of web services, including business services, was initiated when hackers sent an instant message to a single Google employee in China. The instant message linked to a website that enabled hackers to manipulate the employee's personal computer.

Using a *single computer* as an access point, the hackers gained further access to Google's network at its headquarters in California. From there, they accessed a critical software repository that contained the information that they stole. The hackers transferred the stolen information to another set of computers in Texas, and from there to an unknown location. The attack on Google highlights how vulnerabilities in a *single* area within the Internet ecosystem can cause reverberations throughout the *entire* Internet ecosystem.

Exploitation of vulnerabilities can be achieved through any number of access points throughout the Internet ecosystem. Indeed, some of the most newsworthy events in recent years have highlighted the vulnerabilities contained in software (*e.g.*, both the Conficker virus and the recent Sony hack exploited software vulnerabilities),[9] consumer websites (*e.g.*, the recent

[8] See, David E. Sanger, John Markoff, *After Google's Stand on Chine, U.S. Treads Lightly*, New York Times, January 14, 2010 (available at: http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=1&ref=technology) (visited August 1, 2011).

[9] Nick Bilton, New York Times, BITS Blog, *Sony Explains PlayStation Attack to Congress*, May 4, 2011 (available at: http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/?scp=3&sq=sony%20playstation&st=cse (visited August 1, 2011).

Citibank hack utilized the customer website as the gateway),[10] hardware (*e.g.*, acknowledgement that imported electronics are sometimes pre-loaded with malware),[11] and even consumer end users. Once a hacker has breached any of these individual vulnerabilities, its ability to impact other segments of the Internet environment is increased.[12] As a result, any definition the Department adopts must acknowledge the diverse nature of products, services and devices that comprise the Internet.

III. THE DEPARTMENT'S PROPOSED DEFINITION OF I3S OVERLAPS WITH EXISTING DESIGNATIONS

To the extent the Department decides to define a new sector, USTelecom believes that broadband providers should be included in the definition because they are inextricably linked to cybersecurity, and should therefore be included in the Department's definition of the I3S sector.[13] The cybersecurity efforts of broadband providers are both highly relevant and complementary to those of the new sector. USTelecom is concerned, however, that the Department's categorization of I3S does not correspond to existing DHS designations for covered critical infrastructure and could create confusion about the scope of the Department's cybersecurity activities related to non-covered critical infrastructure.

Homeland Security Presidential Directive 7 (HSPD-7) established the national policy for Federal departments and agencies to "identify and prioritize critical infrastructure and to protect

[10] Nelson D. Scwarz, Eric Dash, New York Times, *Thieves Found Citigroup Site an Easy Entry*, June 13, 2011 (available at: http://www.nytimes.com/2011/06/14/technology/14security.html?scp=2&sq=citibank%20hacker&st=cse) (visited August 1, 2011).

[11] Geoff Duncan, Digital Trends, *DHS aware of imported electronics pre-loaded with malware*, July 11, 2011 (available at: http://www.digitaltrends.com/international/dhs-aware-of-imported-electronics-pre-loaded-with-malware/) (visited August 1, 2011).

[12] *See*, New York State Office of Cyber Security website, *Cyber Security Advisories* (available at: http://www.dhses.ny.gov/ocs/advisories/) (visited August 1, 2011).

[13] *Green Paper*, p. 10 (defining the "provision of information services" as being included in the I3S.).

them from terrorist attacks."[14] Pursuant to HSPD-7, each industry's designated sector-specific agency (currently DHS for the IT sector) must collaborate with members of industry to: (a) "identify, prioritize, and coordinate the protection of critical infrastructure and key resources;" and (b) "facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."

According to the IT Sector Coordinating Council, there are a total of six "critical IT sector functions" used to determine whether a service constitutes critical infrastructure. One of these critical functions is providing "Internet-based content, information and communications services."[15] Another critical function is providing "Internet routing, access and connection services."[16] Because both the IT and communications sectors support these covered critical functions, it is unclear how the Department's definition of I3S relates to these existing definitions.

To avoid undue confusion, USTelecom urges the Department to clearly delineate which services and infrastructures are within the scope of the proposed partnership – and do so in a manner that, like DHS designations, recognizes that a wide variety of Internet stakeholders must be addressed for cybersecurity measures to be effective. The suggestions that follow build upon the expectation that industry members and the Department will work together to promote cybersecurity and appropriately define the scope of a potential partnership.

[14] Homeland Security Presidential Directive 7 (available at: (http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm) (visited August 1, 2011).

[15] ITSCC, Fact Sheet, Information Technology Sector Baseline Risk Assessment (available at: http://www.it-scc.org/documents/itscc/ITSRA_Fact_Sheet_FINAL.pdf) (visited August 1, 2011).

[16] *Id.*

IV. BROADBAND PROVIDERS ALREADY ARE INVOLVED IN EXTENSIVE PUBLIC OUTREACH, EDUCATION, AND RESEARCH AND DEVELOPMENT EFFORTS

The Department's green paper identifies three goals in terms of cybersecurity education and research: (1) to develop better cost/benefit analysis for cybersecurity, (2) to measure cybersecurity efforts, and (3) to facilitate research and development for deployable technologies. USTelecom agrees that these goals can help improve cybersecurity efforts. Indeed, USTelecom already participates in the National Initiative for Cybersecurity Education (NICE), through which the Department seeks to coordinate and improve awareness-raising efforts. USTelecom and its member companies have worked continuously to facilitate private sector research of cyber threats, as well as to educate end-users. Through partnerships such as the National Cyber Security Alliance ("NCSA"), for example, our members coordinate with 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 users and protect our shared digital assets.[17]

In addition to extensive public outreach efforts, broadband providers are constantly researching new ways to protect consumers. The USTelecom Cybersecurity Working Group (CSWG), for instance, exemplifies the industry's commitment to promoting cybersecurity due diligence through voluntary private sector efforts, government partnerships, and consumer responsibilities. The CSWG actively monitors and researches existing cybersecurity initiatives and evaluates a variety of new operational solutions that could benefit our members.

[17] *See* National Cyber Security Alliance, *About Us – STAYSAFEONLINE.ORG* (available at: http://www.staysafeonline.org/content/about-us (visited August 1, 2011).

V. THE DEPARTMENT CAN FURTHER PROMOTE CYBERSECURITY BY INCENTIVIZING VOLUNTARY INVESTMENT, INFORMATION-SHARING AND BEST PRACTICES

The Department asks what role it can play in promoting public-private partnerships and how those partnerships can be used to foster better incentives to enhance cybersecurity. In answering these questions, it is important to acknowledge the vast multitude of actors with varying business models and incentives that operate within the Internet ecosystem. These actors include not only Internet Service Providers (ISPs), but also applications and operating system developers, as well as other entities. Among the actors that could be included in the proposed I3S, there is a great disparity in terms of ability, competency, and investment in cybersecurity practices and technologies. While some actors take significant steps to improve cybersecurity, others are less incentivized to do so.[18] The Department should therefore foster increased cybersecurity through funding incentives available to all major actors in the Internet ecosystem. In addition, the Department should facilitate research of current and emerging threats.

A. Companies Have Different Incentives to Share Information and Invest in Cybersecurity

How different companies respond to security threats, and the extent to which they currently invest in cybersecurity, depends largely on their business models. Not all business models place the same emphasis or dedicate sufficient resources to cybersecurity. Because of the Internet's fundamentally interconnected nature, vulnerabilities that arise in one part of the ecosystem can adversely affect all other regions of the Internet. A significant portion of vulnerabilities that threaten users and businesses arise in the application and device layers. In a

[18] *See generally, e.g.*, Comments of AT&T at the FCC, *Cyber Security Certification Program*, PS Docket No. 10-93 (submitted July 12, 2010) ("[S]ubstantial 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.").

recent analysis of enterprise applications by Veracode, researchers found that 57 percent of all applications and 81 percent of third-party software applications had less than acceptable security standards.[19]

The current state of affairs creates serious challenges for network operators, who are often faced with security vulnerabilities originating outside their span of control. For example, when network providers discover problems in operating systems of routers running within core IP networks, remediation efforts are often frustrated when some companies refuse to share information with network operators about known vulnerabilities.

There is no question that broadband providers already have strong market-based incentives to secure their infrastructure. Because broadband providers operate in a highly competitive marketplace, broadband providers' business models are fully dependent on having a secure, resilient and reliable network.[20] Any flaws in broadband providers' infrastructures would result in substantial losses of both customers and revenue. Because of these strong incentives, USTelecom member companies are investing billions of dollars annually to expand and enhance the security of their networks and infrastructure.[21]

[19] 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/soss/executive-summary-veracode-state-of-software-security-report-volume2.pdf) (visited August 1, 2011).

[20] *See e.g.*, Comments of USTelecom at the FCC, *Cyber Security Certification Program,* PS Docket No. 10-93 (submitted July 12, 2010).

[21] *Id.*

B. The Department Should Foster Increased Cybersecurity Through Funding Incentives Available to All Major Actors in the Internet Ecosystem

The Department proposes to work with segments of the private sector to "develop security best practices that can become industry policy standards."[22] In response to this proposal, USTelecom urges the Department to promote cybersecurity by pursuing federal funding initiatives and incentives that benefit all major actors in the Internet ecosystem, such as tax incentives, government procurement, and streamlined regulatory requirements.[23] Due to the inseparable nature of the Internet ecosystem, cybersecurity efforts are unlikely to succeed in the absence of broad industry participation, which must include all major actors and stakeholders.

Although broadband providers play an important role in securing cyberspace, the adoption of best practices by a single segment of the industry would be of very limited benefit.[24] In order for the current state of affairs to improve significantly, the Department needs to ensure the cooperation of other actors, particularly those providing services at the network's edge. As explained in a Concept Paper submitted as part of the White House's 60-day cyber review, "human operators, manufactured and custom computer software, and manufactured computer hardware each contribute more relative vulnerability than does the network infrastructure." [25] Accordingly, the Department should work with the developers of applications and operating systems to facilitate best practices and encourage them to share important security-related information with network operators.

[22] Department of Commerce, *Cybersecurity, Innovation and the Internet Economy*, (available at: http://www.ntia.doc.gov/internetpolicytaskforce) (visited August 1, 2011).

[23] *Green Paper*, p. 23.

[24] *SANS Report*, Vulnerability Exploitation Trends, (available at: http://www.sans.org/top-cyber-securityrisks/) (visited August 1, 2011).

[25] Concept Paper, *National Cyber Systems Infrastructure Security Review*, February 15, 2009, (available at: http://www.whitehouse.gov/files/documents/cyber/Brecht%20Lyle%20-%20NATIONAL%20CYBER%20SYSTEMS%20INFRASTRUCTURE%20SECURITY%20REVIEW%20CONCEPT%20PAPER.pdf) (visited August 1, 2011).

The Department can encourage broad private sector innovation and information-sharing through a variety of financial incentives. The Cross Sector Cyber Security Working Group (CSCSWG),[26] for example, recommends that the government stimulate private sector innovation through direct funding, as well as other measures such as tax incentives for cybersecurity improvement.[27] The Department could support legislation that would provide tax incentives for the development of, and compliance with, adequately robust cybersecurity standards and practices. The Department could also work with other government entities to streamline regulation.

In addition to direct financial incentives, the Department should, to the extent possible, minimize risks associated with proactive cybersecurity practices and information-sharing. As the Department speculated in its *Notice*, current liability structures can create impediments to effective communication between the government and private sector, as well as between different private sector actors. As a result, the parties that are sometimes best situated to remedy a situation are often left in the dark. The White House's Cyberspace Policy Review recommends that the government take measures to "incentiviz[e] collective action and enhance competition in the development of cybersecurity solutions"[28] The report specifically states that the government should explore adjustments to liability considerations, which may include "reduced liability in

[26] The DHS's Cross-Sector Cyber Security Working Group (CSCSWG) provides a forum for exchanging information on common cyber security challenges and issues (i.e., threats, vulnerabilities, and consequences) and enhancing the understanding across sectors of mutual dependencies and interdependencies.

[27] Cross Sector Cyber Security Working Group, Incentives Subgroup, *Incentives Recommendations Report*, September 2009, p. 7-11.

[28] White House Report, *Cyberspace Policy Review*, *Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 28 (available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited August 1, 2011).

exchange for improved security," as well as indemnification.[29] By supporting such changes to current liability structures, the Department can help facilitate the development of more informed cybersecurity solutions and quicker responses to cyber threats.

C. The Department Should Facilitate Research of Current and Emerging Threats

In the *Notice*, the Department asks what new or increased efforts it should undertake to facilitate cybersecurity education and research. Additionally, the Department seeks to identify specific areas where education and research are needed. USTelecom, having an established history of supporting cybersecurity awareness and education efforts, recognizes the importance of cybersecurity education and research.

USTelecom agrees with the Department that improved focus on end-user education should be a primary concern. Industry and government efforts to secure cyberspace, though critically important, are no substitute for basic online safety precautions that can only be taken by end-users. According to a four-year study conducted by Verizon, 87 percent of data breaches could be avoided if users took appropriate steps to protect their devices.[30] Moreover, a study by the Institute for Homeland Security Solutions found that in general Internet users are willing to pay money in order to prevent ISPs from taking measures that would prevent the spread of malware such as botnets.[31] Given these statistics, one potential area of research could be how to incentivize users to care more about cybersecurity or teach them to view assistance by ISPs in a more favorable light.

[29] *Id.* at p. v.

[30] Verizon Business Risk Team, *2008 Data Breach Investigations Report*, 2-3, *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf (visited August 1, 2011).

[31] Institute for Homeland Security Solutions, *2011 Economic Analysis of ISP Provided Cyber Security Solutions*, 27-29 (available at: https://www.ihssnc.org/portals/0/Rowe_IHSS_Cyber_Final_ReportFINAL.pdf) (visited August 1, 2011).

Insofar as the Department wants to become more deeply involved in research and education of particular types of threats, it should consider focusing on anti-botnet initiatives. Although other more dangerous types of malware may exist in the Internet ecosystem, botnets are among the most common threats that directly implicate economic concerns. The Department can lend its support as an important voice in the ongoing collaboration between the private sector and government to curb the spread of botnets, as well as other emerging and future threats. The Department could also examine the implications of the organized criminal behavior known as "hacktivism." As evidenced by the recent attacks against Sony, hacker exploitation of system vulnerabilities has the potential to result in serious damage to our national economy.

VI. CONCLUSION

USTelecom encourages the Department to promote cybersecurity by incentivizing voluntary investment, information-sharing and best practices. Although industry members have different incentives to share information and invest in cybersecurity, the Department can foster better incentives by funding private sector efforts and providing benefits to multiple actors across the Internet ecosystem.

USTelecom looks forward to working with the Department and all major Internet stakeholders to advance cybersecurity education, research, and awareness in order to empower users and improve cybersecurity throughout the Internet ecosystem. Broadband providers are already heavily involved in public outreach, education, and research and development efforts. The Department can promote these efforts by removing disincentives to collaboration and by facilitating research of current and emerging threats through the public-private partnership.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: ____
Robert Mayer
Kevin G. Rupy
Paul Eisler

Its Attorneys

607 14th Street, NW, Suite 400
Washington, DC 20005
(202) 326-7300

August 1, 2011