

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

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

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

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

July 12, 2010

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY..... 1

II. CYBERSECURITY ISSUES REPRESENT A HIGHLY COMPLEX AND RAPIDLY EVOLVING ENVIRONMENT..... 2

III. BROADBAND PROVIDERS ALREADY HAVE SIGNIFICANT INCENTIVES IN THE CYBERSECURITY MARKETPLACE TO ENSURE SECURE INFRASTRUCTURE. 6

IV. PRESCRIPTIVE REGULATION WOULD UNDERMINE THE SUBSTANTIAL BENEFITS RESULTING FROM PUBLIC PRIVATE PARTNERSHIPS..... 7

A. Public-Private Partnerships Have an Established History of Success and Benefits in Addressing Complex Issues..... 7

B. An Effective Public-Private Architecture Has Been Implemented for National Cyber Incident Management and Policy Coordination 10

1. Private and Governmental Entities Have Mechanisms in Place to Prevent, Detect and Respond to the Broad Range of Attacks Occurring in Cyberspace 11

2. The Commission Should Participate in Existing Coordination Efforts in the Cybersecurity Domain 14

V. FEDERAL POLICYMAKERS WOULD BEST PROMOTE ENHANCED CYBERSECURITY WITH GOVERNMENT FUNDING INITIATIVES THAT SUPPORT PRIVATE SECTOR EFFORTS AND BENEFIT ALL MAJOR STAKEHOLDERS IN THE CYBER-ECOSYSTEM. 17

VI. CONCLUSION. 20

* * *

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

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

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

I. INTRODUCTION AND SUMMARY

The United States Telecom Association (USTelecom)¹ is pleased to comment on the Notice of Inquiry (*Notice*)² issued by the Federal Communications Commission (Commission) in the above referenced proceeding. The Internet is a highly complex global system of networks that is constantly evolving and changing. The multiple environments that make up this ecosystem operate on several levels, each of which performs a supporting function for the other levels, thereby implicating the entire network, and by extension the Internet ecosystem itself. As the Internet evolves and changes, the number and complexity of threats throughout the Internet ecosystem likewise transform and change. In addition to managing traditional problems, cybersecurity professionals today must be prepared to respond to highly coordinated and targeted attacks, often committed in discrete areas of the Internet ecosystem.

Private businesses have substantial market-based incentives to invest in, and secure this critical communications infrastructure. Regardless of the type of network platform, private companies' business models are fully dependent on having a secure, resilient, always on and

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 of Inquiry, *Cyber Security Certification Program*, 24 FCC Rcd. 13064, 75 Fed. Reg. 26171 (May 11, 2010) (*Notice*).

reliable network. Any flaws in secure and reliable infrastructures results in private companies losing customers and business.

Responsive efforts and collaboration among Internet stakeholders (*e.g.*, network providers, consumers, consumer electronics and software manufacturers) are essential to ensuring that future cyber threats can be detected and prevented or mitigated effectively. As such, the FCC should support the public-private partnership model as an ideal mechanism for ensuring successful implementation of constructive cybersecurity policies. Such partnership models have a long history of success in other contexts, and it is already producing tangible results in the current cybersecurity environment. Prescriptive regulations could substantially undermine these public-private partnerships by chilling these cooperative efforts between industry and government. To further enhance network integrity in the cybersecurity environment, federal policymakers instead should institute federal funding initiatives that support private sector efforts and benefit *all* major stakeholders in the cyber-ecosystem.

II. CYBERSECURITY ISSUES REPRESENT A HIGHLY COMPLEX AND RAPIDLY EVOLVING ENVIRONMENT

The Internet is a highly complex global system of networks, the compound 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 ecosystem³ through which massive amounts of data is transferred and exchanged. In this sense, the Internet has developed an organic quality

³ See, William B. Norton, The Evolution of the U.S. Internet Peering Ecosystem, November 19, 2003 (available at: <http://dev.nanog.org/meetings/nanog31/presentations/norton.pdf>) (visited July 12, 2010).

insofar as it continually grows and adapts in response to new systems, which are constantly being added to its networks.

The multiple environments that make up this ecosystem operate on several levels, each of which performs a supporting function for the other levels,⁴ thereby implicating the entire network, and by extension the Internet ecosystem itself. Consequently, isolating individual components of the Internet ecosystem is impossible. Furthermore since the Internet has no centralized governance structure, regulating components in one particular environment (*e.g.*, broadband networks) over which regulators have jurisdiction would in no way guarantee the security in other equally important areas (*e.g.*, software providers).

Unfortunately, as the Internet has grown, so have the number and complexity of threats throughout the ecosystem. In addition to managing traditional problems such as denial of service attacks, Trojan horses, worms, and viruses, cybersecurity professionals today must be prepared to respond to highly coordinated and targeted attacks, often committed in discrete areas of the Internet ecosystem. The recent attack on Google and at least thirty-three other companies from an entity in mainland China exemplifies the new breed of cyber attacks that aim to compromise our nation's interests.⁵

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

⁴ See, Computer Engineering, Inc. website, *The Structure of the Internet* (available at: http://www.computerengineering.ca/about_Internet/Internet_structure.php) (visited July 12, 2010).

⁵ See, David E. Sanger, John Markoff, *After Google's Stand on China, 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 July 12, 2010).

linked to a website that enabled hackers to manipulate the employee's personal computer. Using this 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 which contained the stolen information. The hackers transferred the stolen information to another set of computers in Texas, and from there to an unknown location. At the very least, the hackers knew the names of the company's employees beforehand; but they probably also had other information since they gained unauthorized access to Google's internal directory.⁶

The attack on Google highlights how vulnerabilities throughout the Internet ecosystem – including the targeting of specific employees – can be exploited by highly skilled and malicious actors. In some instances, exploitation can be achieved through vulnerabilities in software that run on most computers. For example, the New York State Office of Cyber Security and Critical Infrastructure Coordination publishes a listing of cybersecurity vulnerabilities that includes support programs such as Microsoft Windows Help, the Mozilla web browser and numerous other software products. When these vulnerabilities are exploited, a hacker can install programs, access and change information, and even create new accounts.⁷

Responsive efforts and collaboration among Internet stakeholders (*e.g.*, network providers, consumers, consumer electronics and software manufacturers) are essential to ensuring that future cyber threats can be detected and prevented or mitigated effectively. As such, for the sake of furthering national security and economic objectives, the government

⁶ See, John Markoff, *Cyberattack on Google Said to Hit Password System*, New York Times, April 19, 2010 (available at: http://www.nytimes.com/2010/04/20/technology/20google.html?_r=1) (visited July 12, 2010).

⁷ See, New York State Office of Cyber Security website, *Cyber Security Advisories* (available at: <http://www.cscic.state.ny.us/advisories/>) (visited July 12, 2010).

should encourage and support Internet stakeholders throughout the Internet ecosystem in their continued and consistently improving cybersecurity efforts.

Because stakeholders exist simultaneously and indistinguishably throughout the internet ecosystem, they are better situated than the public sector to secure cyberspace, specifically in terms of their infrastructure and resources, which allow for timely access to critical information. Furthermore, as direct targets of cyber threats and attacks, Internet stakeholders have powerful economic incentives, as well as a collective responsibility, to develop and implement effective cybersecurity measures, and to regularly improve upon such measures. It therefore follows that any successful approach to cybersecurity concerns necessarily involves a coordinated effort among *all* stakeholders in the Internet ecosystem as a collective, and not a mere subdivision thereof.

This understanding is consistent with previous findings that the private sector's collective and shared efforts are essential to securing cyberspace and protecting the national communications infrastructure.⁸ As such, even assuming the Commission has authority to regulate only a segment of the Internet ecosystem, such regulation would likely hinder rather than advance national cybersecurity objectives. That is not to say the Commission, or the public sector more broadly, lacks an important role in securing cyberspace and furthering national cybersecurity objectives; only that its functions and support of cybersecurity initiatives, though equally vital, are inherently different from those of the private sector. Thus, a sound policy is

⁸ See, National Security Telecommunications Advisory Committee Report, *NSTAC Response to the Sixty-Day Cyber Study Group*, March 12, 2009 (*NSTAC Report*).

one that involves increased cooperation between the public and private sectors, in pursuit of commonly shared objectives.

III. BROADBAND PROVIDERS ALREADY HAVE SIGNIFICANT INCENTIVES IN THE CYBERSECURITY MARKETPLACE TO ENSURE SECURE INFRASTRUCTURE.

In the cybersecurity environment, more than 85 percent of the nation's critical infrastructure is owned and operated by private companies.⁹ These private businesses have substantial market-based incentives to invest in, and secure this critical communications infrastructure. Regardless of the type of network platform, private companies' business models are fully dependent on having a secure, resilient, always on and reliable network. Any flaws in secure and reliable infrastructures results in private companies losing customers and business. As a result, businesses today take substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace.

As AT&T noted in testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, “[c]yber-security is a leading corporate priority, and we are investing significant resources in making our network and our customers more secure.”¹⁰ USTelecom member companies are investing billions of dollars annually in expanding the capabilities of their networks and infrastructure as well as to enhance their networks' reliability and security.¹¹

⁹ Rep. Bart Gordon (D-TN), The Hill, *Cybersecurity is National Security*, July 14, 2009 (available at: <http://science.house.gov/press/PRArticle.aspx?NewsID=2609>) (visited July 7, 2010).

¹⁰ See, Statement of Edward Amoroso, Senior Vice President & Chief Security Officer, AT&T Inc., Before the United States Senate Committee On Commerce, Science and Transportation, Hearing on Improving Cybersecurity, p. 3, March 19, 2009 (*Amoroso Testimony*).

¹¹ For example, both AT&T and Verizon have separately acquired businesses that focus on global security issues. See AT&T Press Release, October 1, 2009, *AT&T Acquires VeriSign's Global Security Consulting Business* (available at: <http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=27183>) (visited July 7,

A number of companies have implemented the capability within their networks to automatically detect and mitigate most Distributed Denial of Service Attacks before such nefarious activities affect service to its customers.

IV. PRESCRIPTIVE REGULATION WOULD UNDERMINE THE SUBSTANTIAL BENEFITS RESULTING FROM PUBLIC PRIVATE PARTNERSHIPS

In the cybersecurity context, USTelecom supports the public-private partnership model as an ideal mechanism for ensuring successful implementation of constructive cybersecurity policies. Such partnership models have a long history of success in other contexts, and they are already producing tangible results in the current cybersecurity environment. Prescriptive regulations could substantially undermine these public-private partnerships by chilling these cooperative efforts between industry and government.

A. Public-Private Partnerships Have an Established History of Success and Benefits in Addressing Complex Issues

As noted previously, the cybersecurity environment is a highly complex universe consisting of a global set of stakeholders representing public and governmental entities. In such a complex environment, it would be impossible for a single entity or group of stakeholders (*e.g.*, government entities) to successfully operate independently. Only through cooperation and coordinated efforts can critical goals be successfully attained. Such a cooperative approach has been consistently identified by many key organizations as an essential component of the nation's

2010); *see also*, Verizon Press Release, July 9, 2007, *Verizon Business Completes Cybertrust Acquisition* (available at: <http://investor.verizon.com/news/view.aspx?NewsID=844>) (visited July 7, 2010).

cybersecurity strategy.¹² Fortunately, there is an established history of success under such cooperative models.¹³

More importantly, in the cybersecurity environment there has been exceptional cooperation between public and private entities that have produced tangible and positive results. One of the most relevant – and timely – examples is the successful response by a coalition of public-private entities to the ‘Conficker’ worm.¹⁴ Other examples of close public-private

¹² See e.g., Center for Strategic and International Studies Report, *Securing Cyberspace for the 44th Presidency*, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, December 2008, pp. 43 – 48 (stating that the U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities) (*CSIS Report*) (available at: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf) (visited July 7, 2010); see also, White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. iv (stating that the Federal government should enhance its partnership with the private sector) (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited November 4, 2009) (*White House Cyberspace Policy Review*); see also, Intelligence and National Security Alliance Report, *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*, November 2009, p. 3 (stating that an effective public-private partnership for cyber security would provide the abilities to detect threats and dangerous or anomalous behaviors, to create more secure network environments through better, standardized security programs and protocols and to respond with warnings or technical fixes as needed) (available at: <http://insaonline.org/assets/files/CyberPaperNov09R3.pdf>) (visited July 7, 2010) (*INSA Cyber-Security Report*).

¹³ Outside of the cybersecurity context, there has been a long and successful track record of public-private partnerships. According to the National Council for Public-Private Partnerships (Council), public-private partnerships have been in use in the United States for over 200 years and “thousands are operating today.” See The National Council for Public-Private Partnerships website, *Top Ten Facts About PPPs*, (available at: <http://ncppp.org/presskit/topTen.shtml>) (visited July 7, 2010). Of particular note, the Council states that such partnerships are not only extremely common and an essential tool during challenging economic times, but they also often lead to better public safety. *Id.* On the issue of public safety, the Council notes that “[f]rom Los Angeles to the District of Columbia, local governments have formed creative partnerships with private companies to enhance the safety of its streets and its citizens. By turning over the operation of parking meters or the processing of crime reports to private-sector partners, police officers can spend more time on the streets doing the jobs for which they are trained. This is particularly important as Home Land Security has risen as a concern for many.”

¹⁴ Conficker is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. Conficker has exploited flaws in Windows operating software to take over more than five million computers in more than 200 countries which are then commanded remotely by its authors. Markoff, John, *Defying Experts, Rogue Computer Code Still Lurks*, *New York Times*, August 26, 2009 (available at: <http://www.nytimes.com/2009/08/27/technology/27compute.html>) (visited July 7, 2010). Shortly after Microsoft Corporation announced an alliance of various industry partners to mitigate the Conficker worm, the Department of Homeland Security (DHS) announced the release of a detection tool that can be used by the federal government, commercial vendors, state and local governments, and critical infrastructure owners and operators to scan their networks for the Conficker computer worm. This cooperation was a critical factor in addressing this substantial threat. See Microsoft Press Release, *Microsoft Collaborates With Industry to Disrupt Conficker Worm*, February 12,

partnerships include industry and government participation in the DHS sponsored Cyber Storm Exercises in 2006 and 2008, as well as similar collaboration on the real-world denial of service attacks that occurred during the July 4, 2009 holiday weekend.¹⁵

These types of cooperative efforts between public and private entities are widely embraced by government leaders. As the DHS Secretary Janet Napolitano concluded in a speech on cybersecurity issues, “[t]o be most effective, we in government must work closely with the private sector, and include it in our work as a full partner from the very start.”¹⁶ The Secretary stated that by working in close collaboration these public-private efforts are better able to analyze various threats, “develop strategies to mitigate them, and collaborate on solutions that were fast, widely shared, and compatible at all levels.”¹⁷

President Obama framed his Administration’s policy more emphatically, when he stated, “[s]o let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.”¹⁸

2009 (available at: <http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.msp>) (visited July 7, 2010); See also, DHS Press Release, *DHS Releases Conficker/Downadup Computer Worm Detection Tool*, released March 30, 2009 (*DHS Press Release*). DHS stated that in addition to developing the tool, it was “working closely with private sector and government partners to minimize any impact from the Conficker/Downadup computer worm.”

¹⁵ DHS Blog, July 8, 2009 (available at: <http://www.dhs.gov/journal/theblog/2009/07/morning-roundup-july-8th.html>) (visited July 7, 2010) (discussing a widespread and unusually resilient computer attack that began July 4 knocked out the Web sites of several government agencies, including some that are responsible for fighting cyber crime).

¹⁶ Secretary’s Web Address on Cybersecurity, *A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack*, October 20, 2009 (available at: http://www.dhs.gov/ynews/gallery/gc_1256070988236.shtm) (visited July 7, 2010) (*Napolitano Speech*).

¹⁷ *Napolitano Speech*.

¹⁸ Cross Sector Cyber Security Working Group, Incentives Subgroup, *Incentives Recommendations Report*, September 2009, p. 6 (*CSCSWG Report*).

The proposals included in the Commission’s Notice appear to be inconsistent with President Obama’s policy statement. Specifically, the Commission is seeking to establish a “voluntary incentives-based certification program” in which participating communications service providers would receive network security assessments by government approved auditors who would examine provider’s “adherence to stringent cyber security practices.”¹⁹ Only those providers whose networks “successfully complete the assessment” would be permitted to market their networks as complying with “stringent FCC network security requirements.”²⁰

While couched as a voluntary program, the Commission’s proposal likely would chill participation by industry in the current public-private partnership environment. Industry participants would be justifiably concerned that their collaborative best practices proposals – which often pertain to only certain segments of the industry – would be transformed into “stringent FCC network security requirements.”²¹ Because best practices are not intended as a ‘one-size-fits-all’ solution, their designation by the FCC as a de facto requirement would hinder cooperative efforts between public and private entities.

B. An Effective Public-Private Architecture Has Been Implemented for National Cyber Incident Management and Policy Coordination²²

There currently exists a robust and effective public-private mechanism that is effectively addressing cyber incident management and coordination. These joint efforts are proactively and effectively preventing, detecting and responding to the broad range of attacks that occur in

¹⁹ Notice, ¶12.

²⁰ *Id.*, ¶12.

²¹ *Id.*, ¶12.

²² See, DHS website, The National Strategy to Secure Cyberspace, February 2003, (available at: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf) (visited July 7, 2010).

cyberspace. While the Commission should not seek to duplicate these efforts, USTelecom encourages the Commission to become engaged in these forums as one of the many expert agencies in the cyber realm.

1. Private and Governmental Entities Have Mechanisms in Place to Prevent, Detect and Respond to the Broad Range of Attacks Occurring in Cyberspace

In light of the favorable aspects of public-private partnerships, it should come as no surprise to the Commission that such mechanisms are already in place, and functioning extremely well. Through a broad range of collaborative efforts in the cybersecurity realm, network operators and other private entities are working closely with key stakeholders in the government arena. Indeed, in a report submitted last year to the White House by the National Security Telecommunications Advisory Committee (NSTAC),²³ the group noted that one theme of particular significance was the “continued commitment to foster a strong public/private partnership in order to strengthen our national cybersecurity posture.”²⁴

These partnerships have been so successful, in part, because they are predicated on the mutual sharing of information between industry participants and government stakeholders. This mutual sharing of information is both beneficial and pragmatic for both government and industry

²³ See, NSTAC website, (<http://www.ncs.gov/nstac/nstac.html>) (visited July 7, 2010). For over 25 years, the NSTAC has brought together up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. These industry leaders provide the President with collaborative advice and expertise, as well as robust reviews and recommendations. The NSTAC’s goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture.

²⁴ NSTAC Report, p. 1.

stakeholders since more than 85 percent of the nation's critical infrastructure is owned and operated by private companies.²⁵

These collaborative efforts can be seen in the form of well-established public-private entities, as well as the adoption of key policy documents. Examples of the former include the United States Computer Emergency Readiness Team (US-CERT),²⁶ NSTAC and the DHS Critical Infrastructure Partnership Advisory Council (CIPAC).²⁷ Each of these organizations is populated with key stakeholders from both the government and private sectors,²⁸ and has been operating successfully for several years. Both the US-CERT and CIPAC have been in existence since 2003 and 2006, respectively,²⁹ while for the last 25 years the NSTAC has provided the President with collaborative advice and expertise on matters of telecommunications critical infrastructure.

²⁵ Rep. Bart Gordon (D-TN), The Hill, *Cybersecurity is National Security*, July 14, 2009 (available at: <http://science.house.gov/press/PRArticle.aspx?NewsID=2609>) (visited July 7, 2010).

²⁶ See, US-CERT website, (<http://www.us-cert.gov/>) (visited July 7, 2010). The US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

²⁷ See, CIPAC website, (http://www.dhs.gov/files/committees/editorial_0843.shtm) (visited July 7, 2010). DHS established the CIPAC to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments.

²⁸ For example, among the members of the CIPAC are the Commission, the General Services Administration, the National Association of Regulatory Utility Commissioners, the Department of Commerce, the Department of Defense, DHS, the Department of Justice, Alcatel-Lucent, Association of Public Television Stations, AT&T, Boeing, CTIA - The Wireless Association, Cincinnati Bell, Cisco, Comcast, DirecTV, Embarq, Hughes Network Systems, Internet Security Alliance, Intrado, Juniper Networks, Level 3, National Association of Broadcasters, National Cable & Telecommunications Association, Qwest, Rural Cellular Association, the Satellite Broadcasting and Communications Association, Satellite Industry Association, Sprint Mobile, Telecommunications Industry Association, Tyco, Utilities Telecom Council, US Internet Services Provider Association, USTelecom, VeriSign and Verizon. See DHS website, *Council Members, Critical Infrastructure Partnership Advisory Council*, available at: http://www.dhs.gov/files/committees/editorial_0848.shtm#2 (visited July 7, 2010).

²⁹ See Federal Register Notice, *Critical Infrastructure Partnership Advisory Council*, 71 Fed. Reg. 14930, March 24, 2006 (available at: <http://edocket.access.gpo.gov/2006/06-2892.htm>) (visited July 7, 2010).

In addition to the above public-private partnerships, there are many other such efforts that are working diligently within the confines of this well-established structure.³⁰ These partnerships have resulted in substantive steps that have included implementation of critical policies,³¹ as well as substantive procedures that have been implemented into real-time mechanisms designed to effectively prevent, detect and respond to cyber attacks.³² Many of these existing and well-established frameworks present opportune forums for the Commission to lend its expertise.

³⁰ There are other instances of such public-private partnerships in the cybersecurity context. For example, the 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. The CSCWG has been in existence since May 2007. See e.g., *Statement for the Record*, Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security, Before the United States House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection, October 31, 2007 (available at: <http://homeland.house.gov/SiteDocuments/20071031154922-91266.pdf>) (visited July 7, 2010). Similarly, In January 2000, the National Coordinating Center was designated an Information Sharing and Analysis Center (COMM-ISAC) for communications. The COMM-ISAC facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure. See e.g., National Communications System, *Fiscal Year 2008 Report*, p. 29 (available at: http://www.ncs.gov/library/reports/ncs_fy2008b.pdf) (visited July 7, 2010). In addition, the Communications Sector Coordinating Council (COMM-SCC), with its government partners, works to protect the Nation's communications critical infrastructure and key resources from harm and to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. See, U.S. Communications Sector Coordinating Council website, available at: <http://www.commscc.org/> (visited July 7, 2010).

³¹ Such measures include Homeland Security Presidential Directives (HSPDs) which are a form of executive order issued by the President of the United States. Many HSPDs address matters of critical infrastructure, including those relating to telecommunications. Other examples include the Emergency Support Function #2, Communications Annex (ESF-2), which was issued in January 2008 to "support[] the restoration of the communications infrastructure, facilitate[] the recovery of systems and applications from cyber attacks, and coordinate[] Federal communications support to response efforts during incidents requiring a coordinated Federal response." See, FEMA website, EFS-2, available at: <http://www.fema.gov/pdf/emergency/nrf/nrf-esf-02.pdf> (visited July 7, 2010).

³² See e.g., DHS Press Release, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center*, October 30, 2009 (available at: http://www.dhs.gov/ynews/releases/pr_1256914923094.shtml) (visited July 7, 2010) (*NCCIC Press Release*) (announcing the opening of a 24-hour, DHS-led coordinated watch and warning center that will improve national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure).

2. The Commission Should Participate in Existing Coordination Efforts in the Cybersecurity Domain

There are several significant ways for the Commission to contribute to enhanced protection, detection, mitigation and response to events that occur in the broad cybersecurity ecosystem. First, the Commission should consider its appropriate role in the broader coordination context of cybersecurity efforts. As the Commission has recently acknowledged, its role in the cybersecurity realm “is to complement and support efforts by the Justice and Homeland Security departments.”³³ The Commission also should consider outreach to discrete areas in the cybersecurity environment, specifically the consumer and small business communities to ensure implementation of effective cybersecurity practices.

In the coordination context, the Intelligence and National Security Alliance (INSA) recently noted that in the context of the global cybersecurity environment, “[l]aws, standards and technology cannot simply be levied against such an integrated system of networks. Questions over roles, responsibilities, and jurisdictional boundaries only become more prolific as we strive to clarify them.”³⁴ INSA went on to note that government entities operating in the role of a regulator have the capability to conduct international action and outreach, as well as to incentivize greater participation in cybersecurity efforts.³⁵

As the key regulator over one of the components of the cybersecurity environment, such a role is well suited for the Commission, which can complement existing coordination efforts by

³³ Adam Bender, *FCC Aims to Do More on Cybersecurity*, Communications Daily, November 3, 2009 (noting a statement by Public Safety & Homeland Security Bureau spokesman Robert Kenny that the Commission believes its role is to complement and support efforts by the Justice and Homeland Security departments.).

³⁴ *INSA Cyber-Security Report*, p. 4.

³⁵ *Id.*, p. 6.

other critical agencies. The importance of interagency coordination was recently identified by The White House as a key component to the nation's cybersecurity action plan.³⁶

In this regard, the Commission should consider greater collaboration with existing government cybersecurity related entities including the National Science Foundation and the National Institute of Standards and Technology (NIST)³⁷ Computer Security Division as well as coordination during cyber incident response with the U.S. CERT. The Commission could strengthen its visibility in the recently established National Cybersecurity and Communications Integration Center (NCCIC), which brings together various government organizations responsible for protecting cyber networks and infrastructure and private sector partners.³⁸ The value of these organizations and efforts will be significantly enhanced by the Commission's leadership and expertise in the communications arena.

Regarding outreach efforts, such an approach was identified by the White House as part of its near term action plan.³⁹ Such measures have been successfully implemented by the Commission in the past and are ideally suited in the current context. For example, the

³⁶ See *White House Cyberspace Policy Review*, p. 37 (identifying as a near term action plan the convening of appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulating coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government).

³⁷ The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems. The CSD is a source for substantial expertise related to certifications and accreditations. NIST is currently engaged in various activities that are consistent with areas of expertise inherent in the Commission's ongoing activities. This includes NIST's Smart Grid Interoperability Project, as well as projects relating to cybersecurity. See e.g., NIST Press Release, *Commerce Secretary Unveils Plan for Smart Grid Interoperability*, released September 24, 2009 (available at: http://www.nist.gov/public_affairs/releases/smartgrid_092409.cfm) (visited July 7, 2010); see also, NIST Press Release, *NIST Releases Final Version of New Cybersecurity Recommendations for Government*, released July 31, 2009 (available at: http://www.nist.gov/public_affairs/techbeat/tbx2009_0731_sp800-53iii.htm) (visited July 7, 2010).

³⁸ *NCCIC Press Release*.

³⁹ See *White House Cyberspace Policy Review*, p. 37 (identifying as a near term action plan the initiation of a national public awareness and education campaign to promote cybersecurity).

Commission recently renewed the charter for the Communications Security, Reliability, and Interoperability Council (CSRIC).⁴⁰ The purpose of the CSRIC is to provide recommendations to the Commission to ensure optimal security, reliability, operability and interoperability of communications systems, including public safety, telecommunications, and media communications systems. In this regard, the Commission established Working Group 2A of the CSRIC (Cybersecurity Best Practices). Working Group 2A is currently examining cybersecurity best practices, including those pertaining to all segments of the communications industry and public safety communities.⁴¹ These ongoing public-private efforts are generating tangible results that will further the efforts of industry and government to identify and prioritize the most critical best practices for communications providers to adopt and implement.

Further outreach, particularly to the consumer and small business communities, can be coordinated through the Commission's Consumer and Governmental Affairs Bureau (CGB). The CGB has a long track record of successful outreach in this area, and is well suited for informing consumers and small businesses about critical issues in the cybersecurity context.⁴² For example, the Commission and CGB could focus on raising consumer awareness regarding digital hygiene (*e.g.*, emphasizing the importance of not sharing user identification names or

⁴⁰ See, Public Notice, *FCC Seeks Nominations by May 11, 2009 for Membership on the Communications Security, Reliability, and Interoperability Council (CSRIC)*, DA 09-816, 24 FCC Rcd 4201 (2009).

⁴¹ See, CSRIC website, *CSRIC Working Group Descriptions, Working Group 2A – Cybersecurity Best Practice* (available at: <http://www.fcc.gov/pshs/advisory/csric/wg-2a.pdf>) (visited July 7, 2010).

⁴² The CGB has conducted extensive outreach in several critical areas, including the Rural Health Care Pilot Program, Lifeline and Link-Up, the Do-Not-Call Registry and the digital television transition (*see* CGB website, available at: <http://www.fcc.gov/cgb/>) (visited July 7, 2010).

passwords, password protecting important documents, etc.). One such approach targeted towards children and parents, was announced by the Commission Chairman earlier this year.⁴³

V. FEDERAL POLICYMAKERS WOULD BEST PROMOTE ENHANCED CYBERSECURITY WITH GOVERNMENT FUNDING INITIATIVES THAT SUPPORT PRIVATE SECTOR EFFORTS AND BENEFIT ALL MAJOR STAKEHOLDERS IN THE CYBER-ECOSYSTEM.

Federal policymakers should pursue federal funding initiatives that would enable further private sector innovation and investment throughout the *entire* cyber-ecosystem. As USTelecom has already noted, broadband providers play a complementary – but not exclusive – role in this diverse ecosystem, where the actions of independent entities directly impact other stakeholders in the network. A recent report from the SANS Institute concluded that “the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems.”⁴⁴ In other words, the greatest threat exposure in the cyber ecosystem is at the network’s edge.⁴⁵ This same vulnerability was highlighted in a recent Concept Paper submitted as part of the White House’s 60-day cyber review that addressed the issue of network security.⁴⁶ The report notes that, “[t]he network configuration (*e.g.* Internet or intranet connectivity) is not necessarily the most vulnerable component of the U.S. cyber

⁴³ Prepared Remarks of Chairman Julius Genachowski, Federal Communications Commission, Digital Opportunity: A Broadband Plan for Children and Families, National Museum of American History, Washington, D.C., March 12, 2010 (available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296829A1.pdf) (visited July 10, 2010).

⁴⁴ SANS Institute Report, The Top Cyber Security Risks, September, 2009 (available at: <http://www.sans.org/top-cyber-security-risks/>) (visited July 7, 2010) (*SANS Report*).

⁴⁵ *SANS Report*, Vulnerability Exploitation Trends, (available at: <http://www.sans.org/top-cyber-security-risks/trends.php>) (visited July 7, 2010) (noting that “the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems.”).

⁴⁶ See, 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 July 7, 2010) (*Concept Paper*).

systems infrastructure.”⁴⁷ The report concludes that “human operators, manufactured and custom computer software, and manufactured computer hardware each contribute more relative vulnerability than does the network infrastructure.”⁴⁸

Multiple parties have offered constructive suggestions for how to facilitate new and improved cybersecurity efforts by this wide range of stakeholders. At a hearing this summer of the Subcommittee on Communications, Technology, and the Internet that focused on cybersecurity, Larry Clinton, President of the Internet Security Alliance, outlined a number of steps the government could take to help facilitate this further investment. These included leveraging the purchasing power of the Federal Government; streamlining regulation; and/or reducing complexity and establishing tax incentives for the development of, and compliance with, cybersecurity standards practices and use of technology.⁴⁹

The White House’s cybersecurity report contemplates similar options “for incentivizing collective action and enhance competition in the development of cybersecurity solutions.”⁵⁰ Possible incentives that the report identifies include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification and tax incentives. USTelecom believes that such measures

⁴⁷ *Concept Paper*.

⁴⁸ *Concept Paper*. The Concept Paper notes that “[h]uman operators often are inadequately trained and do not routinely perform even minimal ongoing [operating and maintenance (O&M)] to the software and hardware under their control or use. Even with adequate O&M, some hardware and software is so out-of-date due to lack of timely [repair and replacement], that adequate security cannot be maintained. The fact that this outdated hardware and/or software is connected to the network and that human operators may not address even minimal O&M requirements creates a situation of heightened vulnerability to other network users whether this is a highly secured or unsecured network.”

⁴⁹ Testimony of Larry Clinton, President Internet Security Alliance, House Subcommittee on Telecommunications and the Internet, May 1, 2009 (available at: http://energycommerce.house.gov/Press_111/20090501/testimony_clinton.pdf) (visited July 7, 2010) (*Clinton Testimony*).

⁵⁰ *White House Cyberspace Policy Review*, p. 28.

will help foster an environment that encourages and supports existing incentives for companies to voluntarily adopt widely accepted sound security practices.

This assessment is reinforced by a recent report from the Cross Sector Cyber Security Working Group (CSCSWG) that concludes that government can help facilitate, through an effective incentives program, the broad adoption of sound cyber security practices throughout the Internet ecosystem. The CSCSWG finds that by adopting such incentives, “the power of the market can be harnessed to motivate improved cyber security.”⁵¹

The CSCSWG recommends six incentives for achieving this critical public policy goal.⁵² Among the top three recommendations identified by the CSCSWG are addressing federal government cybersecurity needs, providing grants to accelerate adoption of cybersecurity standards and practices and streamlining/reducing regulatory requirements.⁵³ The group also recommends direct funding for cybersecurity research and development (R&D), grants for cybersecurity R&D and tax incentives for cybersecurity improvement.

USTelecom encourages the Commission to support legislation that would create such incentives. As the CSCSWG concluded, “[t]he recommended incentives taken together as a system of incentives offer the Federal government opportunities to bridge the gap between what private sector’s business plans will support for cyber security investment and what might be needed to satisfy government requirements in different areas.”⁵⁴

⁵¹ *CSCSWG Report*, p. 3.

⁵² *Id.*, pp. 7 – 11.

⁵³ *Id.*, pp. 7 – 8.

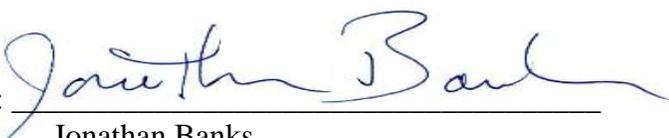
⁵⁴ *CSCSWG Report*, p. 12.

VI. CONCLUSION.

As the Internet evolves and changes, the number and complexity of threats throughout the Internet ecosystem likewise transform and change. USTelecom members place an extremely high value on cybersecurity issues and are voluntarily engaged in existing public-private partnerships, which have proven to be robust and effective mechanisms for ensuring the security of cyberspace. Prescriptive regulations could substantially undermine these public-private partnerships by chilling these cooperative efforts between industry and government. As private businesses continue to invest in, and secure this critical communications infrastructure, federal policymakers should encourage these efforts with federal funding initiatives that would benefit all major stakeholders in the cyber-ecosystem.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: 

Jonathan Banks
Robert Mayer
Kevin Rupy

607 14th Street, NW, Suite 400
Washington, D.C. 20005