

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

)	
In the Matter of)	
)	GN Docket Nos. 09-47, 09-51, 09-137
Additional Comment Sought on Public)	PS Docket Nos. 06-229, 07-100, 07-114
Safety, Homeland Security, and)	WT Docket No. 06-150
Cybersecurity Elements of National)	CC Docket No. 94-102
Broadband Plan, NBP Public Notice # 8)	WC Docket No. 05-196
)	
)	

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

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

November 12, 2009

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY.....	1
II.	PUBLIC-PRIVATE PARTNERSHIPS IN THE CYBERSECURITY REALM ARE PRODUCING TANGIBLE AND POSITIVE RESULTS.....	2
	<i>A. Public-Private Partnerships Have an Established History of Success and Benefits in Addressing Complex Issues</i>	<i>3</i>
	<i>B. An Effective Public-Private Architecture Has Been Implemented for National Cyber Incident Management and Policy Coordination.....</i>	<i>5</i>
	1. Private and Governmental Entities Have Mechanisms in Place to Prevent, Detect and Respond to the Broad Range of Attacks Occuring in Cyberspace.....	6
	<i>C. Significant Incentives Exist in the Cybersecurity Marketplace to Provide Secure Infrastructure to Consumers who Remain Well Informed of Their Competitive Choices in Providers</i>	<i>9</i>
	1. Businesses Have Substantial Market Incentives for Investing in, and Securing, Communications Infrastructure, but the Government Should Further Incentivize Additional Spending	9
	2. Consumers Today Benefit from Numerous Independent Information Resources to Ensure Safe Online Practices	12
	<i>D. Additional Steps are Being Taken to Improve Cybersecurity, but More Can be Done</i>	<i>14</i>
	1. There are a Wealth of Cyber Security Best Practices That Have Been Widely Adopted and Implemented by Communications Providers.....	14
	2. More Can be Done to Improve Cybersecurity, Including Adherence to Specific Standards or Best Practices by all Cyber Ecosystem Participants..	17
	3. The Commission’s Should Participate in Existing Coordination Efforts in the Cybersecurity Domain	17
III.	DEPLOYMENT OF NG-9-1-1 NETWORKS WILL REQUIRE EFFORTS BY VARIOUS STAKEHOLDERS AND DEPLOYMENT OF NEW TECHNOLOGIES.....	20
	<i>A. There are Critical Infrastructure Requirements that must be Satisfied to Ensure Robust Deployment of NG-9-1-1 Networks.....</i>	<i>20</i>
	<i>B. Deployment of NG-9-1-1 Networks Remains in a Nascent, but Promising, Stage</i>	<i>22</i>

1.	Deployment of NG-9-1-1 Networks Remain in a Nascent Stage.....	22
2.	Some Localities have Deployed NG-9-1-1 Networks to a Limited Degree	23
3.	Certain Factors can Encourage Deployment of NG-9-1-1 Networks.....	24
<i>C.</i>	<i>Evolving Technical Standards are Critical to Successful Deployment of NG-9-1-1 Networks.....</i>	<i>26</i>
1.	NG-911 Technical Standards are Being Defined and Developed	26
2.	Ensuring the Secure and Technologically Compatible Interconnection of PSAPs is Critical for NG-9-1-1 Deployment	28
<i>D.</i>	<i>Certain Regulatory Hurdles Exist at the State and National Level.....</i>	<i>30</i>
<i>E.</i>	<i>Public Safety Agencies at the Local, State and Federal Level Will Play a Crucial Role in the Deployment of NG-9-1-1 Networks.....</i>	<i>32</i>
IV.	CONCLUSION	34

* * *

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

)	
In the Matter of)	
)	GN Docket Nos. 09-47, 09-51, 09-137
Additional Comment Sought on Public)	PS Docket Nos. 06-229, 07-100, 07-114
Safety, Homeland Security, and)	WT Docket No. 06-150
Cybersecurity Elements of National)	CC Docket No. 94-102
Broadband Plan)	WC Docket No. 05-196
)	
)	

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

I. INTRODUCTION AND SUMMARY

USTelecom is pleased to provide these comments in the Commission’s above referenced proceeding, regarding aspects of the Federal Communications Commission’s (the Commission) National Broadband Plan that will impact public safety, homeland security and cybersecurity. USTelecom shares the Commission’s view that broadband offers numerous benefits to emergency responders and other public safety agencies that will help them to achieve their respective and diverse missions.¹ USTelecom’s members are particularly focused on aspects of cybersecurity and implementation and deployment of next generation 911 (NG-9-1-1) services.

USTelecom fully supports the nation’s migration of public safety and homeland security services to more advanced offerings that are possible in a broadband environment. USTelecom’s member companies are working diligently to support and implement this migration, which will bring more advanced and robust public safety and homeland security services to the nation.

¹ Public Notice, *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice # 8, DA 09-2133 (released September 28, 2009).

It is imperative that at this critical juncture, the successful migration of public safety and homeland security services to a full broadband-enabled environment does not come at the expense of the security of the nation's broadband networks. Today's cyber ecosystem is a highly complex universe consisting of a global set of stakeholders engaged in a system of multifaceted cooperation designed to facilitate information sharing, reduce vulnerabilities, and to mitigate cyber threats. Telecommunications carriers play a central – but not exclusive – role in this diverse ecosystem, where the actions of independent entities directly impact other stakeholders in the network.

This is exactly the conclusion that was reached in President Obama's recent Cyberspace Policy Review, which noted that "multiple vendors' products are used to configure U.S. telecommunications infrastructure and deliver services ... that cross provider boundaries. As a result of the industry's shift to a horizontal structure and its fragmentation into a large number of firms, neither vendors nor service providers are prepared to take responsibility for end-to-end systems design."² As a result of this architectural reality, carriers' operational capabilities can often be impacted by external players at any point in the network system.

II. PUBLIC-PRIVATE PARTNERSHIPS IN THE CYBERSECURITY REALM ARE PRODUCING TANGIBLE AND POSITIVE RESULTS

In the cybersecurity context, USTelecom supports the public-private partnership model as an ideal mechanism for ensuring successful implementation of constructive cybersecurity

² See, White House Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, p. 41 (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited October 28, 2009) (*White House Cyberspace Policy Review*) (quoting Robert Lucky and Jon Eisenberg, editors, Committee on Telecommunications Research and Development, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, *Renewing U.S. Telecommunications Research*, 2006, at 36-37 (available at: http://sites.nationalacademies.org/cstb/CompletedProjects/CSTB_042246) (visited October 28, 2009).

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. Under such a cooperative model, private companies have strong incentives to provide robust and secure network services to consumers, and these companies continue to improve existing security features.

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 cybersecurity strategy.³ Fortunately, there is an established history of success under such cooperative models.

³ 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 November 4, 2009); 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 November 4, 2009) (*INSA Cyber-Security Report*).

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),⁴ public-private partnerships have been in use in the United States for over 200 years and “thousands are operating today.”⁵ 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.⁶

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.⁷ Shortly after Microsoft Corporation announced an alliance of various industry partners to mitigate the Conficker worm,⁸ the Department of Homeland Security (DHS) announced the release of a detection tool that can be used by the

⁴ The National Council for Public-Private Partnerships is a non-profit, non-partisan organization founded in 1985. According to its website, the Council is “a forum for the brightest ideas and innovators in the partnership arena.” Its growing list of public and private sector members, with experience in a wide variety of public-private partnership arrangements, and its diverse training and public education programs represent vital core resources for partnering nationwide. The Council’s members bring an unmatched dedication to providing the most productive and cost-effective public services.

⁵ See The National Council for Public-Private Partnerships website, Top Ten Facts About PPPs, (available at: <http://ncppp.org/presskit/topten.shtml>) (visited October 27, 2009).

⁶ *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.”

⁷ 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 October 27, 2009).

⁸ Along with Microsoft, organizations involved in this collaborative effort include the Internet Corporation for Assigned Names and Number (ICANN), NeuStar, VeriSign, CNNIC, Afiliias, Public Internet Registry, Global Domains International Inc., M1D Global, AOL, Symantec, F-Secure, ISC, researchers from Georgia Tech, the Shadowserver Foundation, Arbor Networks and Support Intelligence. See Microsoft Press Release, *Microsoft Collaborates With Industry to Disrupt Conficker Worm*, February 12, 2009 (available at: <http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.msp>) (visited October 27, 2009).

federal government, commercial vendors, state and local governments, and critical infrastructure owners and operators to scan their networks for the Conficker computer worm.⁹ This cooperation is ongoing and has been a critical factor in addressing this substantial threat. Other examples of close public-private 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.¹⁰

These types of cooperative efforts between public and private entities are widely embraced by government leaders. As the DHS Secretary Janet Napolitano recently noted 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.”¹¹ As the Secretary noted, 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.”¹²

B. An Effective Public-Private Architecture Has Been Implemented for National Cyber Incident Management and Policy Coordination¹³

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

⁹ See 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.”

¹⁰ DHS Blog, July 8, 2009 (available at: <http://www.dhs.gov/journal/theblog/2009/07/morning-roundup-july-8th.html>) (visited November 5, 2009) (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).

¹¹ 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 October 27, 2009) (*Napolitano Speech*).

¹² *Napolitano Speech*.

¹³ See The National Strategy to Secure Cyberspace, February 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, last visited October 9, 2009.

effectively preventing, detecting and responding to the broad range of attacks that occur in 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 Occuring 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 recent report submitted to The White House by the National Security Telecommunications Advisory Committee (NSTAC),¹⁴ 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.”¹⁵

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

¹⁴ See, NSTAC website, (<http://www.ncs.gov/nstac/nstac.html>) (visited October 27, 2009). 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.

¹⁵ NSTAC Report, March 12, 2009.

stakeholders since more than 85 percent of the nation's critical infrastructure is owned and operated by private companies.¹⁶

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),¹⁷ NSTAC and the DHS Critical Infrastructure Partnership Advisory Council (CIPAC).¹⁸ Each of these organizations is populated with key stakeholders from both the government and private sectors,¹⁹ and has been operating successfully for several years. Both the US-CERT and CIPAC have been in existence since 2003 and 2006, respectively,²⁰ while for the last 25 years the NSTAC has provided the President with collaborative advice and expertise on matters of telecommunications critical infrastructure.

¹⁶ 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 October 28, 2009).

¹⁷ See, US-CERT website, (<http://www.us-cert.gov/>) (visited October 27, 2009). 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.

¹⁸ See, CIPAC website, (http://www.dhs.gov/files/committees/editorial_0843.shtm) (visited October 27, 2009). 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.

¹⁹ 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 October 27, 2009).

²⁰ See Federal Register, <http://edocket.access.gpo.gov/2006/06-2892.htm>.

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.²¹ These partnerships have resulted in substantive steps that have included implementation of critical policies,²² as well as substantive procedures that have been implemented into real-time mechanisms designed to effectively prevent, detect and respond to cyber attacks.²³ Many of these existing and well-established frameworks present opportune forums for the Commission to lend its expertise.

²¹ 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 October 28, 2009). 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 October 28, 2009). 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 October 28, 2009).

²² 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 October 28, 2009).

²³ 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 November 5, 2009) (*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).

C. Significant Incentives Exist in the Cybersecurity Marketplace to Provide Secure Infrastructure to Consumers who Remain Well Informed of Their Competitive Choices in Providers

As previously noted, in the cybersecurity environment more than 85 percent of the nation's critical infrastructure is owned and operated by private companies.²⁴ These private businesses have substantial market-based incentives to invest in, and secure this critical communications infrastructure. Moreover, consumers today have a wealth of information at their fingertips to help them assess the security offerings from all providers of this critical resource.

1. Businesses Have Substantial Market Incentives for Investing in, and Securing, Communications Infrastructure, but the Government Should Further Incentivize Additional Spending.

There are strong incentives for private businesses to ensure the security of their network 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 recently noted in testimony before the United States 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.”²⁵

²⁴ 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 October 28, 2009).

²⁵ 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 (available at: <http://commerce.senate.gov/public/ files/TestimonyofEdAmoroso31709.pdf>) (visited October 28, 2009) (*Amoroso Testimony*).

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.²⁶ Some 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.

But as USTelecom has already noted, telecommunications carriers play a central – 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.”²⁷ In other words, the greatest threat exposure in the cyber ecosystem is at the network's edge.²⁸ This same vulnerability was highlighted in a recent Concept Paper submitted as part of the White House 60 day cyber review that addressed the issue of network security.²⁹

The report noted that, “[t]he network configuration (*e.g.* Internet or intranet connectivity) is not necessarily the most vulnerable component of the U.S. cyber systems infrastructure.”³⁰

The report concluded that “human operators, manufactured and custom computer software, and

²⁶ 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 November 4, 2009); 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 November 4, 2009).

²⁷ SANS Institute Report, *The Top Cyber Security Risks*, September, 2009 (available at: <http://www.sans.org/top-cyber-security-risks/>) (visited November 5, 2009) (*SANS Report*).

²⁸ *SANS Report*, *Vulnerability Exploitation Trends*, (available at: <http://www.sans.org/top-cyber-security-risks/#trends>) (visited November 5, 2009) (noting that “the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems.”).

²⁹ 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 October 28, 2009) (*Concept Paper*).

³⁰ *Concept Paper*.

manufactured computer hardware each contribute more relative vulnerability than does the network infrastructure.”³¹

To address this issue, USTelecom encourages government stakeholders to spur innovation and investment in the *entire* cyber-ecosystem. 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 spur 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.³²

Government can and should encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad scale investment to critical infrastructure and key resources through carefully targeted incentives for industry stakeholders. This is the same conclusion reached in The White House’s cybersecurity report, which stated that “[t]he Federal government should consider options for incentivizing collective action and enhance competition in the development of cybersecurity solutions.”³³ 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

³¹ *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.”

³² 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 October 28, 2009) (*Clinton Testimony*).

³³ *White House Cyberspace Policy Review*, p. 28.

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

2. Consumers Today Benefit from Numerous Independent Information Resources to Ensure Safe Online Practices

In this challenging cyber-environment, it is important that consumers have adequate information to make educated decisions about their network services and online activities. Fortunately, substantial independent information exists today for consumers at all levels – including residential and enterprise customers – to make informed decisions on which security measures are available.

Once again, the efforts of the government and private sectors are fulfilling an important role in educating and protecting consumers. Perhaps the best example of this can be seen in the public-private partnership that resulted in the ‘onguardonline.gov’ website. The website – which was developed with the assistance of 12 government agencies (including the Commission)³⁴ and 18 private organizations³⁵ – provides practical tips from the federal government and the technology industry to help consumers be on guard against Internet fraud and secure their

³⁴ In addition to the Commission, other government website partners include the Federal Trade Commission, U.S. Department of Justice, Office of Justice Programs, Department of Homeland Security, Internal Revenue Service, United States Postal Inspection Service, Department of Commerce, Technology Administration, Securities and Exchange Commission, Naval Criminal Investigative Service, U.S. Army Criminal Investigation Command, Federal Deposit Insurance Corporation and the Commodity Futures Trading Commission. *See*, About Us, OnGuardOnline website, <http://www.onguardonline.gov/about-us/overview.aspx> (visited October 28, 2009).

³⁵ Private partners include GetNetWise, National Cyber Security Alliance, Anti-Phishing Working Group, i-SAFE, AARP, National Consumers League, Direct Marketing Association, WiredSafety.org, The SANS Institute, The National Association of Attorneys General, Better Business Bureau, NetFamilyNews, The Computing Technology Industry Association (CompTIA), National Crime Prevention Council, Association of College Unions International, Latinos in Information Sciences and Technology Association, StopBadware.org and iKeepSafe.org. *Id.*

computers personal information.³⁶ The benefits of this website to consumers were recently heralded in a joint press release by the Commission and the Federal Trade Commission,³⁷ as well as in a video statement by President Barack Obama.³⁸

Additional information is also provided to consumers in numerous private publications and resources. These include periodic updates by Consumer Reports (including a robust guide to online security),³⁹ as well as several other consumer related publications such as CNET.

The impacts these resources are having on consumer behavior are clearly positive. A recent report from Norton found that “99% of those surveyed say they take steps to secure their personal information.”⁴⁰ In addition, another study from the Pew Internet & American Life Project (Pew) surveyed 578 leading Internet experts regarding the future of the Internet. In its survey, Pew found that 78% of experts agreed with the statement that “security, and reliability on the Internet are easier and more refined.”⁴¹

³⁶ See, OnGuardOnline Website, available at: <http://www.onguardonline.gov/default.aspx> (visited October 28, 2009).

³⁷ Joint Federal Trade Commission & Federal Communications Commission Release, *FCC and FTC Chairmen Jointly Encourage the Public to Take Safeguards to Protect Themselves, Their Privacy, and Their Personal Information Online*, October 9, 2009 (available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293921A1.pdf) (visited November 9, 2009).

³⁸ The White House Blog, *Protecting Yourself Online*, October 15, 2009 (available at: <http://www.whitehouse.gov/blog/Protecting-yourself-online>) (visited November 9, 2009).

³⁹ See, Consumer Reports Online Security Guide, available at: <http://www.consumerreports.org/cro/electronics-computers/resource-center/cyber-insecurity/cyber-insecurity-hub.htm> (visited October 28, 2009).

⁴⁰ Norton Online Living Report 09, p. 6 (available at: <http://www.nortononlineliving.com/>) (visited October 28, 2009).

⁴¹ Pew Future of the Internet III study, p. 6. An earlier study by Pew in 2005 found that “91% of internet users say they have made at least one change in their online behavior to avoid unwanted software programs.” Pew Internet & American Life Project Report, Susannah Fox, Associate Director, Digital Strategy, *Spyware and the threat of unwanted programs being secretly loaded onto computers are becoming serious threats online*, July 2005, p. 3 (*Pew Study*). Among the changes undertaken by consumers, Pew found that: 1) 81% of internet users say they have stopped opening email attachments unless they are sure these documents are safe; 2) 48% of internet users say they have stopped visiting particular Web sites that they fear might deposit unwanted programs on their computers; 3) 25% of internet users say they have stopped downloading music or video files from peer-to-peer networks to avoid getting unwanted software programs on their computers; and 4) 18% of internet users say they have started using a different Web browser to avoid software intrusions. *Pew Study*, p. 3.

D. Additional Steps are Being Taken to Improve Cybersecurity, but More Can be Done

Communications providers are also taking additional steps to improve network security.

While many carriers are adopting and implementing cybersecurity best practices, the Commission should promote increased consumer and small business education and outreach in the cybersecurity domain.

1. There are a Wealth of Cyber Security Best Practices That Have Been Widely Adopted and Implemented by Communications Providers

Adoption of best practices is a critical component for ensuring secure networks.

Fortunately for carriers seeking information regarding best practices in the cybersecurity environment, there is a wealth of resources available to them. For example, the Commission addresses cybersecurity issues through its Network Reliability and Interoperability Council (NRIC). The NRIC is a former federal advisory committee composed of private sector representatives that catalogue proven operational best practices for carrying out network engineering, monitoring, and maintenance functions. Although the NRIC has been superseded by the Communications Security, Reliability, and Interoperability Council (CSRIC), the Commission correctly notes that the NRIC's cyber security best practices remain available and "are increasingly relevant."⁴²

The Commission's website includes a searchable database for various best practices, including those relating to cybersecurity.⁴³ Of the best practices that are available through the Commission's website, more than 230 address cybersecurity, including those relating to

⁴² Public Safety and Homeland Security Bureau website, *Tech Topic 20: Cyber Security and Communications*, available at: <http://www.fcc.gov/pshs/techttopics/techttopics20.html> (visited October 29, 2009).

⁴³ NRIC Best Practices website, available at: <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm> (visited October 29, 2009) (*Best Practices Website*).

protection against denial of service attacks,⁴⁴ protection of the domain name system from poisoning,⁴⁵ and surveillance of the network.⁴⁶

USTelecom also notes that the Commission recently appointed several individuals to serve on the CSRIC, and renewed its charter through March 18, 2011.⁴⁷ Some of the key activities permitted under the CSRIC charter include recommending best practices and actions the Commission can take to ensure the security, reliability, operability, and interoperability of public safety communications systems; recommending best practices and actions the Commission can take to improve the reliability and resiliency of communications infrastructure; and evaluating ways to strengthen the collaboration between communications service providers and public safety entities during emergencies.

USTelecom believes the renewal of the CSRIC's charter is a prudent step for the Commission to take, and encourages its work on identifying relevant and voluntary best practices.⁴⁸ This is not to say that the Commission should put itself in a position of developing and/or dictating standards or best practices to the private sector. Given the constantly evolving and rapidly changing nature of the cybersecurity threat, a regulatory-standards or best practices based regime will simply not work in such an environment. Rather, the Commission and other

⁴⁴ See, *Best Practices Website*, Detailed Information for the Best Practice: 7-6-8047 (available at: <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-6-8047>) (visited October 29, 2009).

⁴⁵ See, *Best Practices Website*, Detailed Information for the Best Practice: 7-6-8048 (available at: <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-6-8048>) (visited October 29, 2009).

⁴⁶ See, *Best Practices Website*, Detailed Information for the Best Practice: 7-7-0401 (available at: <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-7-0401>) (visited October 29, 2009).

⁴⁷ See Public Notice, FCC Announces Membership of the Communications Security, Reliability, and Interoperability Council (CSRIC), DA 09-2297 (October 26, 2009).

⁴⁸ USTelecom notes that the CSRC does not currently have representatives from the IT sector. As noted previously, USTelecom believes it is important to have all relevant stakeholders throughout the cyber ecosystem involved in these discussions, and we encourage the Commission to include IT representatives in this group's efforts.

governmental stakeholders are better suited to act as central repositories for collecting and disseminating appropriate – and more timely – best practices and standards.

In addition, other resources regarding public and private security practices are available through the National Institute of Standards and Technology (NIST). NIST proactively invites public and private organizations to submit their information regarding security practices for inclusion in its Computer Security Resource Center (CSRC). NIST encourages this broader sharing of such information in order to enhance the overall security of the nation, and covers a broad range of cybersecurity topics.⁴⁹

International standards and practices also fulfill a key component of cybersecurity measures. The International Telecommunications Union (ITU) launched the Global Cybersecurity Agenda (GCA) on 17 May 2007, which is designed as an international framework for cooperation and response and focuses on building partnership and collaboration between all relevant parties in the fight against cyber threats.⁵⁰ Through a series of various working groups and initiatives, the ITU develops and maintains security outreach material, coordinates security-related work, and identifies needs and assignment and prioritization of work to encourage timely development of cybersecurity recommendations.⁵¹

⁴⁹ Nominated candidate policies and procedures may be submitted to NIST in any area of information security including, but not limited to: accreditation, audit trails, authorization of processing, budget planning and justification, certification, contingency planning, data integrity, disaster planning, documentation, hardware and system maintenance, identification and authentication, incident handling and response, life cycle, network security, personnel security, physical and environmental protection, production input/output controls, security policy, program management, review of security controls, risk management, security awareness training, and education (to include specific course and awareness materials), and security planning. See, NIST CSRC website, *Information Technology Security*, available at: <http://www.csrc.nist.gov/pcig/ppsp.html> (visited October 29, 2009).

⁵⁰ See, ITU website, *Cybersecurity Gateway*, available at: <http://www.itu.int/cybersecurity/gateway/> (October 29, 2009).

⁵¹ See e.g., ITU website, *Lead study group on telecommunication security*, available at: <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html> (visited October 29, 2009).

2. More Can be Done to Improve Cybersecurity, Including Adherence to Specific Standards or Best Practices by all Cyber Ecosystem Participants

There are numerous best practices and standards for all participants in the cyberspace environment to adhere to in order to minimize cybersecurity risks. Independent research demonstrates that when companies follow well-established practices of security, they dramatically reduce the effects of attempted cyber incursions.⁵² A recent study by Verizon found that 87% of known system breaches could have been avoided if reasonable security controls had been in place.⁵³ Encouraging such behavior can be accomplished in different ways.

For example, the government could develop an incentive program that rewards implementation of best practices and standards. Such a mechanism would motivate good actors in the business community to take the necessary steps towards further improving cybersecurity. Such an approach was recently recommended in The White House's Cyberspace Policy Review.⁵⁴

3. The Commission's 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

⁵² *Clinton Testimony*, p. 5. Clinton notes that a recent survey conducted by PricewaterhouseCoopers found that organizations that followed best practices had reduced downtime and financial impact, despite being targeted more often by malicious actors. *Id.*

⁵³ Verizon Business Risk Team Report, *2008 Data Breach Investigations Report*, 2008, p. 3 (available at: <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>) (visited October 29, 2009).

⁵⁴ *White House Cyberspace Policy Review*, p. 15.

Homeland Security departments.”⁵⁵ The Commission should also 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.”⁵⁶ 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.⁵⁷

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 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.⁵⁸

In this regard, the Commission should consider greater collaboration with existing government cybersecurity related entities including the National Science Foundation and NIST⁵⁹

⁵⁵ 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.).

⁵⁶ *INSA Cyber-Security Report*, p. 4.

⁵⁷ *INSA Cyber-Security Report*, p. 6.

⁵⁸ 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).

⁵⁹ 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 project relating to cybersecurity. See e.g., NIST Press Release, *Commerce Secretary Unveils Plan for Smart Grid Interoperability*, released September 24, 2009 (available at:

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.⁶⁰ 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.⁶¹ Such measures have been successfully implemented by the Commission in the past and are ideally suited in the current context. For example, the Commission recently rechartered the CSRIC, which will recommend best practices that the government and the communications sector can implement to ensure the security of cyberspace.⁶² 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.⁶³

http://www.nist.gov/public_affairs/releases/smartgrid_092409.html) (visited November 5, 2009); *see also*, NIST Press Release, *NIST Releases Final Version of New Cybersecurity Recommendations for Government*, released July 24, 2009 (available at: http://www.nist.gov/public_affairs/techbeat/tbx2009_0731_sp800-53iii.htm) (visited November 5, 2009).

⁶⁰ *NCCIC Press Release*.

⁶¹ *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).

⁶² *See* Letter from Nneka Ezenwa, Executive Director, Federal Regulatory Affairs, Verizon, to Marlene H. Dortch, dated October 1, 2009, regarding A National Broadband Plan for our Future (GN Docket No. 09-51). USTelecom agrees with Verizon that the Commission should not mandate best practices, however, because such mandates will not keep up with evolving threats.

⁶³ 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 November 5, 2009).

III. DEPLOYMENT OF NG-9-1-1 NETWORKS WILL REQUIRE EFFORTS BY VARIOUS STAKEHOLDERS AND DEPLOYMENT OF NEW TECHNOLOGIES

NG-9-1-1 technology is best described as a multimedia, IP based technology that has a different operating structure than existing 911 Networks. As a recent report from the Congressional Research Service noted, such a communications network of the future is envisioned as IP-based, using standardized protocols, and providing a nationwide overlay of system links that can operate at the national, regional, tribal, state, or local level to best meet the needs of specific circumstances.⁶⁴ The report noted that such a network, “if fully realized, could support many types of emergency communications needs, including first responder networks and emergency alerts.” Clearly, the benefits of a robust NG-9-1-1 network are immeasurable.

But in order for such an important system to be implemented, it will be imperative that all government and private industry stakeholders at the local, state and federal level work in close coordination. The presence of such coordination will be essential to implementing successful deployment of NG-9-1-1 Networks. Another important factor that must be addressed in any successful deployment are those relating to critical infrastructure and implementation of new standards and technologies, some of which have yet to be developed.

A. There are Critical Infrastructure Requirements that must be Satisfied to Ensure Robust Deployment of NG-9-1-1 Networks

NG-9-1-1’s basis on IP networking standards provides numerous advantages, including increased responsiveness, enhanced communications and greater access to information.

However, this same architecture also exposes the network to many of the vulnerabilities associated with today’s public Internet. Security must play a key role in NG-9-1-1 deployment

⁶⁴ Linda K. Moore, Specialist in Telecommunications Policy, Congressional Research Service, *Emergency Communications: The Future of 911*, June 16, 2009, p. 1 (911 Report).

which must be accomplished in such a way as to protect the system against some of the same challenges and malicious acts found on the Internet today. Protecting the integrity of the system is of paramount importance for all involved stakeholders, and security will need to be multifaceted and implemented at multiple levels.

The Department of Transportation (DOT) currently has oversight of NG-9-1-1 deployment. In this regard, DOT has published technical requirements and a concept of operations for NG9-1-1, has implemented a strategic outreach plan, has begun work to develop and validate requirements for the NG9-1-1 system, has defined the system architecture, and has developed a preliminary transition plan. In its concept of operations, DOT notes that “[t]he security of and authorized access to the NG9-1-1 system is *critical* to ensuring that the NG9-1-1 system of systems is secure from security breaches and illegal users to prevent disruption of the delivery of a 9-1-1 call and public safety response to emergencies.”⁶⁵

Any NG-9-1-1 system must be designed to provide security policy for the network infrastructure and resources, as well as to ensure legitimate access, authentication, and authorization for the users of the system. The critical nature of the services offered and privacy concerns of the data make this network attractive for misuse. The network must be highly controlled to ensure service, yet flexible enough to provide open access. USTelecom believes, however, that if the Internet can exist today and remain available to the public, the NG-9-1-1 system should be able to leverage some of its best practices and diverse vendor community to accomplish its mission.

⁶⁵ Intelligent Transportation Systems, U.S. Department of Transportation, *Next Generation (NG9-1-1) System Initiative, NG9-1-1 Preliminary Transition Plan*, April, 2008, p. 31 (*NG9-1-1 Transition Plan*) (emphasis added).

B. Deployment of NG-9-1-1 Networks Remains in a Nascent, but Promising, Stage

At this early stage in NG-9-1-1 deployment, there are promising signs of progress. In limited areas of the country, key stakeholders have engaged in testing of this new technology. Other localities continue to experiment with various aspects of NG-9-1-1 deployment. It is imperative that at this nascent stage, key stakeholders take steps to encourage and nurture more widespread deployments.

1. Deployment of NG-9-1-1 Networks Remain in a Nascent Stage

As part of its assessment of NG-9-1-1 deployment, the DOT recently completed proof of concept testing for such networks. Completed in 2008, the proof of concept testing provided valuable information to all stakeholders regarding the promises and potential of NG-9-1-1 networks.

Specifically, starting in early 2008, DOT conducted NG-9-1-1 testing in seven locations: King County, Washington, Helena, Montana, Saint Paul, Minnesota, Rochester, New York, Indiana PSAP, Texas A&M Laboratory and the Booz Allen CNSI Laboratory.⁶⁶ The testing focused on various aspects of selected requirements for NG-9-1-1 networks, including: 1) the ability to receive voice, video, text (IM, SMS) and data; 2) support for deaf/hearing-impaired accessibility; 3) caller's location identification; 4) transmitting telematics data (Advanced Automatic Crash Notification) like speed, vehicular rollover, crash velocity; 5) call routing based on caller's location; and 6) IP networking and security.⁶⁷

⁶⁶ See, DOT website, *NG-9-1-1 System Initiative, Proof of Concept Testing Report*, available at: http://www.its.dot.gov/ng911/pubs/NG911_POC_TestReport_FINAL091708.htm#7_Demonstration_Testing (visited October 29, 2009).

⁶⁷ Presentation, Intelligent Transportation Systems, U.S. Department of Transportation, *U.S. DOT Next Generation 9-1-1 Project: A National Framework and Deployment Plan*, p. 9 (DOT Presentation).

The results of this testing gave rise to cautious optimism for stakeholders. The group tested 116 functional requirements across three laboratories and five public safety answering points (PSAPs). There were 320 individual tests conducted, with 280 (87.5%) successfully passing the test criteria.⁶⁸ Among the findings by DOT, they received “very positive feedback” from participants, and the test helped to create a “sense of urgency and movement within the community to get more involved and to start discussing the issues.”⁶⁹

Upon completion of this testing, DOT has moved onto the next phase of its implementation, which focuses on transition planning. This phase of its transition planning focuses on various transition issues, including funding, operations, standards and technology, governance and policy, as well as education. DOT is also examining deployment approaches, which analyze either an independent/unilateral approach (i.e., bottom up), or coordinated/intergovernmental approach (i.e., top down).⁷⁰ Because NG-9-1-1 is an always evolving and highly complex technology, it will be imperative for stakeholders to remain engaged throughout the entire transition process.

2. Some Localities have Deployed NG-9-1-1 Networks to a Limited Degree

As stakeholders continue to plan for wider NG-9-1-1 deployment, some states and localities are taking tentative steps into this realm. While in some instances these deployments do not reflect full NG-9-1-1 capabilities, they are nevertheless illustrative of the march of 911 technology towards an IP-based environment.

⁶⁸ *DOT Presentation*, p. 11.

⁶⁹ *DOT Presentation*, p. 11.

⁷⁰ *DOT Presentation*, p. 13.

For example, according to the National Emergency Number Association (NENA), there are various instances of real world applications of NG-9-1-1 deployments. At the state level, there are next generation network projects in process today in Indiana, Montana, Vermont, Rhode Island, Texas, Florida and Minnesota. Smaller scale next generation network implementations are taking place in Washington DC and Allegheny County, Pennsylvania.⁷¹

Moreover, the vast majority of states are either considering or implementing an IP network in preparation for NG-9-1-1.⁷² For example 21 states (or localities within states) have IP networks planned, 9 states have IP networks at the sub-state level, and two states have NG-9-1-1 preparation activity at the state or sub-state level.⁷³ As these individual state efforts mature, states should actively engage stakeholders prepare and plan for the implementation of a full NG-9-1-1 system.

3. Certain Factors can Encourage Deployment of NG-9-1-1 Networks

At this important state of NG-9-1-1 deployment, there are several critical factors that will encourage full and successful deployment. Most critical to ensuring successful deployment of NG-9-1-1 networks are the availability of adequate funding (particularly at the local and state level), as well as coordination amongst all governmental and industry stakeholders at the local, state and federal level. There exists an opportunity for appropriate federal agencies to take a leadership role by emphasizing the need to work closely with state authorities to coordinate planning, information-sharing, and other steps.

⁷¹ NENA Presentation, Next Generation 9-1-1 – The Future for Emergency Communications, p. 47 (*NENA Presentation*).

⁷² See NENA website, NG9-1-1 Project: Status of NG9-1-1 Related IP Networks, Demos and Trials, available at: <http://www.nena.org/ng911-project/ip-network-status> (visited October 30, 2009) (*NENA Status Website*).

⁷³ *NENA Status Website*.

In the funding context, a recent Congressional report found that “[a]mong the multiple factors and challenges of implementing NG9-1-1 are the costs of planning, replacing, and upgrading systems, and maintaining and operating these new systems.”⁷⁴ Current State and local 9-1-1 funding and planning legislation and authority are functionally tied to the architecture of current 9-1-1, and often do not take into consideration funding of NG-9-1-1. As noted recently by NENA, “[a]bsent significant inter-governmental cooperation, this form of planning and funding may not lead to economies of scale that will enable parity of emergency services capabilities, interoperability, increased efficiency or cost savings within all aspects of emergency communications.”⁷⁵ Among other things, both the Congressional report and NENA focused on the role that grants should play in the deployment of NG-9-1-1 networks.⁷⁶

A chief concern expressed by emergency communications managers and others is the need for greater coordination of planning for NG9-1-1 among the states, to maximize benefits such as interoperability, system resilience through shared resources, and economies of scale.⁷⁷ As NENA noted in a report on the issue, “[t]he evolution from today’s 9-1-1 service structure to tomorrow’s [NG-9-1-1] system requires several major areas of simultaneous and interactive activities. A coordinated set of actions combining national, state, and local authorities is required to successfully accomplish critical preparations, development, testing and implementation of NG9-1-1.”⁷⁸

⁷⁴ Congressional Research Service Report, *Emergency Communications: The Future of 911*, p. 16, June 16, 2009 (CRS Report) (available at: http://assets.opencrs.com/rpts/RL34755_20090928.pdf) (visited November 9, 2009).

⁷⁵ NENA Report, *A Policy Maker Blueprint for Transitioning to the Next Generation 9-1-1 System, Issues and Recommendations for State and Federal Policy Makers to Enable NG9-1-1*, September, 2008, p. 6 (NENA Policy Report).

⁷⁶ CRS Report, p. 16, NENA Policy Report, p. 6.

⁷⁷ CRS Report, p. 10.

⁷⁸ NENA Policy Report, Appendix A, p. 12.

USTelecom agrees that jurisdictional frameworks for NG-9-1-1 at the federal, state and local levels must be clarified and implemented, to ensure appropriate nationwide deployment and management. The evolution to full NG-9-1-1 deployment must be treated as a national project in which individual state action is necessary, but must be appropriately coordinated with other state and national activities.

C. Evolving Technical Standards are Critical to Successful Deployment of NG-9-1-1 Networks

As with any major technological development such as NG-9-1-1, standard setting will play a critical role in deployment of this new service. Developing, coordinating, promulgating and maintaining standards enable a wide base of users – including those outside the standards development organization – to adopt and implement uniform applications. These standards will be essential to seamlessly supporting communications and data transfer across county, state, and international borders, and across the multitude of emergency response professions and agencies, from traditional PSAPs to disaster management centers. Widespread of adoption of NG-9-1-1 standards will be essential to ensuring nationwide deployment of these critical services.

1. NG-911 Technical Standards are Being Defined and Developed

Currently, various technical standards for NG-9-1-1 are in varying stages of development, with some critical standards already published, and others in various stages of development. These standards are currently being developed through consensus-based efforts by, among others, NENA, the Internet Engineering Task Force (IETF) and the Emergency

Services Interconnection Forum (ESIF).⁷⁹ It is expected that the end results of these consensus efforts will form the foundation for NG9-1-1 initiative engineering and demonstration projects.

In general, NENA has identified various ‘building blocks’ that are critical for development of NG-9-1-1 standards. These include Emergency Services IP Network (ESInets), international standards, databases and data management and security.⁸⁰ NENA also identifies the general development and support areas that it is focusing on for these efforts.⁸¹ Vendors who are involved in the standards development process “can and are starting to produce NG911 oriented products.”⁸² While this progress is indeed encouraging, NENA also notes that “a fully featured, truly ‘standards based’ NG911 system is not yet identifiable, because the necessary standards are still in development.”⁸³ Nevertheless, fully featured, standards based NG911 will likely be implemented in successive releases.⁸⁴

These ongoing efforts recently came to fruition at a three-day event designed for vendors of NG-9-1-1 system components to test for interoperability with applications, products, and systems produced by other vendors in the NG-9-1-1 arena.⁸⁵ The first of its kind Industry Collaboration Event (ICE), hosted by NENA, involved 16 leading suppliers of NG9-1-1 components who tested their products based on draft and final standards developed by NENA’s Technical Committees, the IETF and other standards development organizations. According to

⁷⁹ Research and Innovative Technology Administration, *Next Generation 9-1-1 System Preliminary Concept of Operations*, p. 1, December 2005 (available at: http://www.its.dot.gov/ng911/next_gen_911_sys.htm) (visited November 10, 2009) (*RITA Report*).

⁸⁰ NENA Article, *What is NG911*, EMS1.com, September 8, 2009 (available at: <http://www.ems1.com/ems-products/communications/articles/588619-What-is-NG911/>) (visited November 10, 2009) (*NENA Article*).

⁸¹ See NENA Development and Support Areas Table, available at: <http://www.ems1.com/data/NENA-table.jpg> (visited November 10, 2009).

⁸² *NENA Article*.

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ NENA Press Release, *NENA, Leading 9-1-1 Vendors Demonstrate Next Generation Capabilities at Industry Collaboration Event*, November 6, 2009 (*NENA Press Release*).

NENA, the ICE enabled vendors to test and validate their implementation of NG-9-1-1 functional elements called for in various standards in an open, collaborative, and supportive forum. NENA intends to continue these efforts, which USTelecom believes will prove instrumental in ensuring widespread and successful deployment of NG-9-1-1 systems.

2. Ensuring the Secure and Technologically Compatible Interconnection of PSAPs is Critical for NG-9-1-1 Deployment

As noted in a recent Congressional Research Service Report (CRS Report) regarding the future of 911 networks, “today’s 911 system is built on an infrastructure of analog technology that does not support many of the features that most Americans expect are part of an emergency response.”⁸⁶ The CRS Report goes on to note that “efforts to splice newer, digital technologies onto this aging infrastructure have created points of failure where a call can be dropped or misdirected, sometimes with tragic consequences.”⁸⁷ Although the general public assumes that the newer technologies they are using to place 911 calls are matched by the same level of technology at the PSAP, the CRS Report correctly concludes that “[t]his is not the case.”⁸⁸ For this reason, USTelecom maintains that a key component for NG-9-1-1 deployment will be the interconnection of all existing PSAPs to broadband networks.

In comments submitted to the Commission in its National Broadband Plan proceeding, NENA states that it is important that the Commission “place a clear priority in the National Broadband Plan on the need for investment in the infrastructure, services and applications for safety organizations that will enable their effective and vastly expanded use of broadband

⁸⁶ *CRS Report*, Summary page.

⁸⁷ *CRS Report*, Summary page.

⁸⁸ *CRS Report*, Summary page.

networks.”⁸⁹ More specifically, NENA states that “there has been insufficient focus on connecting the approximately 100,000 emergency response agencies in America to secure and redundant broadband networks.”⁹⁰ USTelecom agrees that the Commission should take steps to ensure that all PSAPs are connected to broadband services sufficient for NG-9-1-1 and emergency communications.

In addition, it is imperative that the interconnection of PSAPs addresses and emphasizes the security needs for these networks in the broader cybersecurity context. Despite the many advances and capabilities that NG-9-1-1 networks offer, as with any IP-based network, next-generation emergency calling networks could be susceptible to computer viruses and hackers trying to infiltrate and disrupt the system. While securing NG-9-1-1 networks may prove challenging, it is clearly an attainable goal. These issues were recently addressed in NENA’s ICE, where some panelists concluded that such threats are manageable and are being addressed through the continuing release of updated standards.⁹¹

As DOT noted in its 2008 Transition Plan, access to emergency services provided by PSAPs in today’s world of evolving technology “will ultimately occur within a broader array of interconnected networks comprehensively supporting emergency services.”⁹² This interconnection will likely occur over a mix of commercial and government owned network infrastructure. As such, commercial and government-owned broadband networks will be a critical component to any fully deployed NG-9-1-1 network.

⁸⁹ Comments of the National Emergency Numbering Association, National Broadband Plan, GN Docket No. 09-51, p. 2 (June 8, 2009) (*NENA Comments*).

⁹⁰ *NENA Comments*, p. 6.

⁹¹ See e.g., Donny Jackson, *Security for Next-Generation PSAPs*, Urgent Communications, November 9, 2009 (available at: <http://urgentcomm.com/psap/news/ng-911-psap-security-20091109/>) (visited November 10, 2009).

⁹² DOT 2008 Transition Plan, p. 1.

The Commission should therefore work to ensure that this essential interconnection of PSAPs to broadband networks takes place. As addressed in great detail by NENA, there are numerous existing 911 and public safety grant and loan programs in place today that should be leveraged to achieve this interconnection goal.⁹³ For example, NENA notes that programs exist within the Commission, DHS, DOT, the National Telecommunications and Information Administration (NTIA) and the Rural Utilities Service (RUS) to achieve this crucial goal. USTelecom encourages the Commission to coordinate the use of these programs for NG-9-1-1 deployment.

D. Certain Regulatory Hurdles Exist at the State and National Level

In today's 911 marketplace, LECs are the main source of 9-1-1 services. As the NG-9-1-1 marketplace expands and develops, however, it is anticipated that there will be multiple providers offering a variety of service capabilities and options. While an open and competitive NG-9-1-1 environment should be fostered, it is imperative that existing regulations and laws are adequately updated to address the realities of the marketplace.

Many state and federal laws and regulations were written in an era where the technological capabilities of NG-9-1-1 were simply not envisioned. In some instances, existing laws and regulations make specific reference to older technologies or system capabilities which may inadvertently inhibit the migration to NG-9-1-1. It is crucial that state and federal legislatures and regulatory bodies review current laws and regulations to keep pace with this rapidly changing technology and marketplace in order to create a framework that will help foster a competitively neutral marketplace that allows NG-9-1-1 networks and services to flourish.

⁹³ See *NENA Comments*, pp. 13 – 14.

In a recent policy paper regarding recommendations for state and federal policy makers to enable NG-9-1-1 deployment, NENA identified various actions to resolve this regulatory hurdle issue. As NENA noted at the time, “[t]o meet the objective of a fully functioning [NG-9-1-1] and emergency communications system, it is critical that state regulatory bodies and legislatures, as well as the [Commission] and Congress take timely and carefully considered action to analyze and update existing 9-1-1 rules and regulations to ensure they optimize 9-1-1 governing authority choices for E9-1-1 and [NG-9-1-1] and foster competition by establishing a competitively neutral marketplace.”⁹⁴

Among other things, NENA recommends that state legislatures and regulatory bodies, as well as the Commission and Congress, initiate efforts to understand how current regulations and laws facilitate, or inhibit, the local, state, regional and national interoperable environment of NG9-1-1. Examples that NENA offers for examination include laws or regulations concerning the eligible use of 9-1-1 funds; provisions that require specific technology components for “E9-1-1” service delivery that are not necessarily the same for NG-9-1-1; laws that may inhibit appropriate and efficient information sharing of 9-1-1 data with appropriate safeguards for privacy protection; and uniform requirements for all 9-1-1 service providers to meet accepted industry standards (reference to industry standards is necessary for service integrity).⁹⁵ NENA also recommends that where regulatory requirements are in place, such requirements should be functional and performance based without reference to any specific proprietary technologies, manufactures or service providers.

⁹⁴ *NENA Policy Report*, p. 11.

⁹⁵ *NENA Policy Report*, p. 11.

E. Public Safety Agencies at the Local, State and Federal Level Will Play a Crucial Role in the Deployment of NG-9-1-1 Networks

When Congress passed the ENHANCE 911 Act of 2004, it stated that “[e]nhanced 9-1-1 is a high national priority, and it requires Federal leadership, working in cooperation with state and local governments and with the numerous organizations dedicated to delivering emergency communications services.”⁹⁶ In the context of NG-9-1-1, DOT recently noted that “[w]ithout focus and leadership at a national level, NG9-1-1 could face challenges in realizing its goal of a national interconnected system.”⁹⁷ In this regard, the Federal government will play a critical role in fostering migration of public safety agencies at the state and local level to implementation of national-level NG-9-1-1 services.

It will be imperative that with involvement of so many stakeholders in the public and private sector at the Federal, State and local level, that the roles and responsibilities for the deployment of NG-9-1-1 services be defined across jurisdictional boundaries and between new partnerships. Early and continued participation in NG-9-1-1 planning by all relevant stakeholder groups is critical to successfully deploying NG-9-1-1 Networks. As DOT concluded in its Transition Plan, national level coordination must continue and expand in preparation for NG-9-1-1 and other components of the larger next generation emergency communications system.

In its comments regarding the Commission’s National Broadband Plan, NENA recommends that a key principle in the Commission’s plan should be to foster public/private collaboration and coordination at the local, state and national levels.⁹⁸ NENA addresses at length what will be necessary at the state level to organize, plan, coordinate and implement any NG-9-

⁹⁶ PL 108-494, known as the ENHANCE 911 Act of 2004.

⁹⁷ DOT Transition Plan, p. 15 (February 2009).

⁹⁸ *NENA Comments*, p. 6.

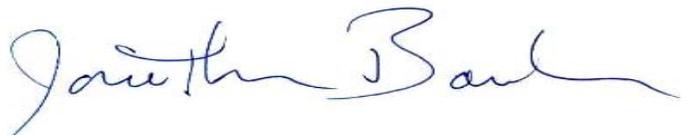
1-1 system,⁹⁹ and USTelecom believes that many of these recommendations are relevant and sound.

⁹⁹ *NENA Comments*, Appendix, pp. i-ii.

IV. CONCLUSION

Broadband offers numerous benefits to emergency responders and other public safety agencies that will help them to achieve their respective and diverse missions. Key building blocks for enhancing our nation's public safety and homeland security efforts will include focusing on issues relating to cybersecurity and implementation and deployment of NG-9-1-1 services. In the cybersecurity context, the successful migration of public safety and homeland security services to a full broadband-enabled environment can be accomplished through successful public-private partnerships, but should not come at the expense of the security of the nation's broadband networks. The deployment of robust NG-9-1-1 services will require involvement by a diverse group of stakeholders, as well as the development and deployment of new technologies. While deployment of these services remains in a nascent stage, the early results are promising. Nevertheless, key government stakeholders can – and should – implement certain initiatives to encourage deployment of these NG-9-1-1 services.

Respectfully submitted,



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