Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
Comments—Public Safety and Homeland Security Bureau Seeks Comment on Whether the Commission's Rules Concerning Disruptions to Communications Should Apply to Broadband Internet Service Providers and Interconnected Voice over Internet Protocol Service Providers	)	**ET Docket No. 04-35** **WC Docket No. 05-271** **GN Docket Nos. 09-47, 09-51, 09-137**

COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION

The United States Telecom Association (USTelecom)[1] is pleased to comment on the Public Notice (*Notice*)[2] issued by the Federal Communications Commission (Commission) in the above referenced proceeding. USTelecom's member companies play a critical role in the nation's communications infrastructure, and each places an extremely high value on the reliability of their service and on minimizing service disruptions. Among other things, these companies incorporate redundancy into their broadband networks to ensure that residential and business customers enjoy uninterrupted service of the highest quality, and work closely with joint government-industry initiatives tasked with ensuring increased network reliability. Broadband network providers have demonstrated a strong commitment to supporting a highly reliable critical infrastructure capable of providing consumers with emergency services in times of national emergency, local disaster, and public health crises.

---

[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] Public Notice, *Public Safety and Homeland Security Bureau Seeks Comment on Whether the Commission's Rules Concerning Disruptions to Communications Should Apply to Broadband Internet Service Providers and Interconnected Voice Over Internet Protocol Service Providers*, DA 10-245 (July 2, 2010) (*Notice*).

Nonetheless, while USTelecom believes that ensuring the continued reliability of broadband networks is of utmost importance, any proposals to expand reporting requirements at this time are unnecessary. In particular, the Commission must consider whether such broadband outage reporting would be counter productive, as they would duplicate existing U.S. Department of Homeland Security (DHS) programs and national policies that currently address similar issues.[3]

I. NETWORK PROVIDERS ALREADY TAKE SUBSTANTIAL STEPS TO ENSURE RESILIENT BROADBAND NETWORKS

Mandatory outage reporting requirements are unnecessary. Such requirements would impose significant, unnecessary, and wasteful burdens on the broadband industry.

As noted in other related proceedings at the Commission, broadband providers take substantial steps to engineer robust mechanisms and procedures into their broadband networks that ensure substantial resiliency and reliability.[4] USTelecom member companies have spent hundreds of millions of dollars to deploy robust broadband networks that are tremendously reliable and increasingly resilient.[5] Ensuring their ability to maintain high quality, uninterrupted

---

[3] *See*, HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection (December 2003). HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure/key resources (CI/KR). HSPD-7 identified Telecommunications and IT as distinct sectors and assigned oversight for both to the DHS. Specifically, HSPD-7 charges the DHS with maintaining an organization—NCSD—to serve as a focal point for the security of cyberspace and facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. The NCSD mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. To the extent permitted by law, Federal departments and agencies with cyber expertise, including the Departments of Justice, Commerce, Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support NCSD in accomplishing its mission.

[4] *See* Comments of the United States Telecom Association in the Matter of Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan (GN Docket Nos. 09-47, 09-51, 09-137) at pp. 9-10.

[5] *See Id.*; *see also* Comments of the United States Telecom Association in the Matter of Framework for Broadband Internet Service (GN Docket No. 10-127) at pp. 4-5.

service is of paramount importance to USTelecom members and acts as a huge incentive for ensuring resiliency in their broadband networks.

USTelecom recently highlighted the substantial and extensive measures taken by its members in order to ensure resilient broadband networks.[6] These substantial measures make perfect sense, since private companies' business models are fully dependent on having a secure, resilient and reliable network. Flaws in reliable infrastructure result in private companies losing customers and business. As a result, businesses are taking substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace. Such guarantees in level of service are routinely embodied in service level agreements (SLAs) between network providers and enterprise customers.

Even during major catastrophic events, the reliability of the nation's broadband networks has been proven time and again. For example, the Department of Homeland Security (DHS) Communications Sector-Specific Plan (CSSP) stated that while the events of September 11, 2001, and the hurricanes of 2005 "highlighted the importance of communications to public health and safety, to the economy, and to public confidence," these disasters "proved the overall resiliency of the national communications network."[7] The report noted that "[d]espite the enormity of these incidents, the network backbone remained intact."[8] Further buttressing this point, a recent report from the Government Accountability Office found that while the discussion

---

[6] *See* Comments of the United States Telecom Association in the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload (PS Docket No. 10-92) at pp. 10-15.
[7] *See*, DHS Report, *Communications, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan*, p. 5, May 2007 (available at: http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf) (visited August 2, 2010) (*Communications SSP*).
[8] *Id.*

of resiliency in some Sector-Specific Plans (SSPs) was somewhat limited, discussion of resiliency in the communications SSP was "relatively extensive."[9]

With more than 85 percent of the nation's critical infrastructure owned and operated by private companies,[10] there are substantial market-based incentives to invest in and secure broadband infrastructure. These critical investments by network operators not only ensure redundancy within the network, but also ensure the implementation of robust practices and processes that allow these businesses to react more rapidly during times of crisis, thereby ensuring the viability and survivability of the network.

II. IP-BASED NETWORKS ARE PART OF A LARGER ECOSYSTEM THAT DOES NOT LEND ITSELF TO TRADITIONAL NETWORK OUTAGE REPORTING

IP Networks differ significantly from the traditional PSTN in terms of structure and complexity. These architectural differences are most evident when contrasting the PSTN's highly-structured hierarchical architecture with the dynamic and distributed architecture of current IP networks.

The hierarchical design of the PSTN was intended to provide for simplistic alternative routing. If a call could not be handled by one level of the structured hierarchy, it would be transferred to the next, thus providing the requisite degree of reliability. Traditionally there were five levels in the ordered hierarchical system, which established direct connections between centralized points. As the PSTN became increasingly ordered in terms of hierarchy, their overall

---

[9] GAO Report, *Critical Infrastructure Protection, Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296, pp. 24-25, March 2010.
[10] 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 August 2, 2010) (*Cybersecurity Article*).

structure became more centralized. The opposite is true of IP Networks, which have grown increasingly diversified and complex throughout their developmental history.

In the current IP network, the data that makes up a communication is derived from an upper level protocol that encapsulates said data (*i.e.* separates it from its underlying structure on basis of logical function) into packets that can be handled meaningfully through a complex and multifaceted process. Unlike the PSTN, which require a circuit to be set up for each phone call, IP networks operate using a connectionless protocol that allows for circuit-less communications between hosts and users across multiple platforms. Thus, in contrast to the simple centralized hierarchy of the PSTN, IP networks are nonhierarchical and highly decentralized.

These design characteristics make it impractical to associate network disruptions with any particular communications or application element. Accordingly, any reporting mechanism designed to address IP outages will, by design, only capture a small slice of a much larger network ecosystem – and provide a skewed view of the source and frequency of outages. Decentralized, non-hierarchical, autonomous systems-based networks simply do not lend themselves to traditional regulated legacy reporting systems.

But should the Commission unwisely pursue reporting requirements for IP-based networks, it is essential that great care is taken to establish clear definitions that capture inherent flexible response mechanisms. Furthermore, disruptions that result from either physical or logical occurrences in other parts of a largely unregulated ecosystem must be included before any meaningful analysis can be undertaken.

III. EXISTING MECHANISMS AT THE FEDERAL LEVEL ARE ALREADY IN PLACE FOR ADDRESSING BROADBAND NETWORK ISSUES

USTelecom has commented at length on DHS-led public-private mechanisms already in place which focus on a broad range of issues including those relating to reliability of broadband networks.[11] These joint efforts are proactively and effectively addressing areas where imposition of broadband outage reporting would be counter-productive and an unnecessary drain on resources. The Commission should not seek to duplicate these efforts, but should instead become engaged in these forums as one of the many expert agencies that can lend a valuable voice of expertise.

Numerous benefits stem from such public-private partnerships, which further enhance the resiliency and dependability of broadband networks.[12] These partnerships have been so successful in part, because they are predicated on the mutual sharing of information between industry participants and government stakeholders who represent a broad span of organizations within DHS and across the federal government. This mutual sharing of information is both beneficial and pragmatic for both government and industry stakeholders since more than 85 percent of the nation's critical infrastructure is owned and operated by private companies.[13] Public-private efforts are successful due to the multi-stakeholder coordination that occurs in addressing challenging issues, in contrast to independent actions taken in a vacuum by individual stakeholders.

---

[11] *See* Comments of the United States Telecom Association in the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload (PS Docket No. 10-92) at pp. 2-10.
[12] *See, e.g., Id.*
[13] *Cybersecurity Article*.

Indeed, the collaboration that occurred to develop the Commission's Disaster Information Reporting System (DIRS) data collection exemplifies the desirable results than can be better achieved through public-private partnerships and cooperation. DIRS is a voluntary information service that allows providers to report on service outages during disasters and national emergencies. Throughout its development and testing phases, DIRS benefited from the expertise of industry professionals, who maintained an understanding of the Commission's expectations, while at the same time assisting the Commission in developing a program that facilitates collaboration among the private and public sectors. Through this collaboration, the Commission has gained access to critical information while maintaining a voluntary process.

As evidenced by this successful collaboration, a mandatory reporting requirement is unnecessary and contrary to a formula that has already been proven to yield favorable results. Instead of imposing mandatory requirements, federal policymakers within and outside of the Commission should work collaboratively with broadband providers to analyze information on outages affecting IP-based networks and to help prevent future outages and ensure a better response to actual outages.

In this regard, DHS is the agency best situated for leading broadband network resiliency and outage issues. In fact, during the Commission's earlier proceeding regarding mandatory Part 4 outage reporting requirements, DHS emphasized that: 1) voluntary reporting is more appropriate; and 2) the National Communications System (NCS) was the appropriate agency for receiving such reports. In particular, DHS expressed its support for voluntary reporting

programs, as opposed to mandatory requirements.[14] DHS also emphasized its trust in the telecommunications industry's efforts to continually improve its reporting systems and invite participation from government agencies in furtherance of their shared goals.[15] Broadband network providers are particularly committed to working towards these goals, as well as to the expansion of public-private efforts to realize them efficiently.

Moreover, DHS already has substantial infrastructure and resources in place for developing appropriate mechanisms. In particular, DHS's National Infrastructure Protection Plan (NIPP) unifies the Nation's Critical Infrastructure and Key Resource (CIKR) protection efforts through its coordinated public-private partnership framework. The NIPP is an essential mechanism for ensuring the greatest possible coordination between government and the private sector.

A noteworthy consideration in this regard is the highly sensitive nature of outage reports and the experience necessary to make use of such information effectively and securely. In the past, DHS has expressed concern that outage information relevant to indentifying and mitigating system vulnerabilities could be exploited by hostile actors who aim to harm communications networks.[16] DHS and broadband providers themselves have significant experience analyzing, securing, and implementing this information. As such, the Commission should avoid its solitary broadband outage reporting approach, and instead coordinate with DHS and other relevant stakeholders through the NIPP process.

---

[14] Comments of the Department of Homeland Security, New Part 4 of the Commission's Rules Concerning Disruptions to Communications (ET Docket No. 04-35), pp. 10 – 11.
[15] *Id.* at 9.
[16] *Id.* at 3.

Another important venue where such coordination and information sharing takes place is the National Security Telecommunications Advisory Committee (NSTAC).[17] 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.

In a recent issues report released by the NSTAC, the group evaluated the role of the National Coordinating Center (NCC) regarding its "mission, information sharing procedures, and overall effectiveness as changes occur in the threat, policy, and technological environments facing the telecommunications industry."[18] The NCC is a joint industry and government center which, operating under the auspices of the National Communications Systems (NCS), Department of Homeland Security (DHS), ensures the timely delivery of resources and technologies to restore critical communications services following an emergency. Additionally, the NCC-ISAC which consists of many communications companies and is housed within the NCC and facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure . The NSTAC concluded in its report, among other things, that there should be

---

[17] *See*, NSTAC website, (http://www.ncs.gov/nstac/nstac.html) (visited August 2, 2010).
[18] NSTAC Report, *Issue Review, A Comprehensive Review of Issues Addressed Through May 2009*, p. 114 (available at: http://www.ncs.gov/nstac/reports/2009/2008-2009%20NSTAC%20Issue%20Review.pdf) (visited August 2, 2010) (*NSTAC Issue Review*).

"better delineation of roles and responsibilities [among telecommunications planning and incident response entities], especially with regard to data reporting" if such delineation would "improve incident response" and "reduce duplication of effort."[19] As explained above, the impositions of mandatory reporting requirements on broadband providers would not improve incident response and would actually create duplication of effort. Thus, the NSTAC recent issues report offers further evidence for why the Commission should not adopt new reporting requirements.

The Commission's *Notice* acknowledges the importance of broadband networks on a national scale and proposes to impose broadband outage requirements similar to those in place for voice and/or paging communications over wireline, wireless, cable and satellite communications services.[20] Such a proposal, however, also runs counter to the findings of DHS in its National Sector Risk Assessment Results Report, which found that disruptions to wireline networks pose an "*insignificant risk to national communications*."[21]

IV. CONCLUSION

In consideration of the aforementioned, USTelecom urges the Commission to refrain from rulemaking or other actions that would expand its Part 4 rules. Broadband providers have strong incentives to ensure their networks are resilient and they have continually taken substantial steps to that effect. Moreover, providers have knowledge and expertise in dealing with IP-based networks, which are part of a larger ecosystem that does not lend itself to traditional outage reporting. The federal policymakers should take advantage of service

[19] *NSTAC Issue Review*, p. 114.
[20] *Notice*, p. 1.
[21] Department of Homeland Security Report, *National Sector Risk Assessment Results Report*, April 2008, p. 40 (emphasis in original).

providers' expertise and work with them to help prevent future outages and ensure a better response to actual outages. Lastly, the Commission should not seek to duplicate, and potentially undermine, existing efforts of agencies with mechanisms already in place to achieve the Commission's intended purpose. Instead, the Commission should become more substantially engaged in collaborative forums with members of industry and other expert agencies, through which it can receive valuable input and better achieve its security and efficiency objectives without unnecessarily burdening the industry.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: _____

Jonathan Banks
Robert Mayer
Kevin Rupy
Paul Eisler

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