Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	**)**	
	)	
Effects on Broadband Communications Networks	**)**	**PS Docket No. 10-92**
Of Damage to or Failure of Network Equipment	**)**	
Or Severe Overload	**)**	
	)	

COMMENTS OF THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

Thomas Goode
ATIS
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

Attorney for ATIS

June 25, 2010

TABLE OF CONTENTS

Summary

ATIS notes that the increasing dependence on broadband services demonstrates that the broadband networks are reliable. Significant work has been completed and more is underway to further enhance network reliability by the industry, both individually and through organizations such as ATIS. ATIS therefore urges the Commission to collaborate with the industry in the development of standards and specifications aimed at fostering network reliability, rather than establishing regulatory mandates that may chill on-going industry work.

While broadband networks are reliable, ATIS notes that no network can be designed or implemented to withstand every possible source of failure. Despite the diligent efforts of service providers, there are circumstances that may result in a loss of service. The network is most vulnerable to points of failure in the last mile from the customer premise to the network's edge. However, while the edge is more vulnerable than the core, failures in the edge affect fewer customers. Even at the core, failures would be less likely to result in blocked service than in the traditional public switched telephone network.

One way in which service providers enhance the reliability of their networks is through the implementation of Best Practices. Best Practices, including physical security practices, are widely deployed by the industry as appropriate. ATIS believes that the success of Best Practices stems from their voluntary nature and urges the Commission not to impose unnecessary regulatory mandates on the use of these practices.

Another way in which providers enhance reliability is by utilizing geographic and component redundancy in their networks. Before equipment is deployed, a detailed evaluation and site survey process is undertaken that includes a review of transport facility availability and diversity. Such diversity means that instances in which all available paths fail would be rare, and would likely be the result of a cataclysmic event. Nevertheless, it should be noted that in the last mile it is difficult to deploy diverse equipment.

ATIS notes that the capacity of residential access networks is sufficient to handle sudden surges in use. However, sustained, unexpected traffic from the entire service population would result in congestion and lowered average throughput speeds for customers. In the event of congestion, service providers have a range of network management solutions. In many cases, the impact of these management tools will be imperceptible to individual users and these users will not experience service impacts.

ATIS believes that the Commission has a significant role in promoting network reliability and should : (1) support and promote awareness of industry-developed standards and Best Practices; (2) continue to partner with industry forums such as the ATIS Network Reliability Steering Committee to identify issues around which the development of Best Practices would be beneficial; and (3) explicitly recognize and support the ability of industry to develop, implement and revise Best Practices according to business requirements.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	**)**	
	)	
Effects on Broadband Communications Networks	**)**	**PS Docket No. 10-92**
Of Damage to or Failure of Network Equipment	**)**	
Or Severe Overload	**)**	
	)	

COMMENTS

The Alliance for Telecommunications Industry Solutions (ATIS) hereby submits these comments in response to the April 21, 2010, *Notice of Inquiry (NOI)*, in the above-referenced docket. In the *NOI*, the Commission seeks to enhance its understanding of the survivability of broadband communications networks. These comments reflect significant input from the ATIS Network Reliability Steering Committee (NRSC), as well as input from the ATIS Next Generation Interconnection Interoperability Forum (NGIIF) and Sustainability in Telecom: Energy and Protection Committee (STEP)**.** ATIS notes that the increasing reliance on broadband services demonstrates that broadband networks are reliable. While ATIS supports the Commission’s efforts to gain a better understanding regarding network survivability, it urges the Commission to “do no harm” to the work underway in the industry to foster reliability and survivability.

I. Introduction

ATIS is a global standards development and technical planning organization that leads, develops and promotes worldwide technical and operations standards for information, entertainment and communications technologies. The development of technical and operations standards is done by industry subject matter experts in ATIS' 18 open industry forums and committees, which focus on issues ranging from the fundamental elements of communications to network reliability and interoperability to the seamless delivery of converged services.

As a developer of standards and specifications that govern both existing and emerging networks, ATIS is pleased to have an opportunity to provide input on the *NOI*. ATIS believes that any Commission examination of network reliability and survivability must as an initial matter acknowledge on-going industry work. Individually and through standards development groups such as ATIS, communications companies strive to provide their customers with reliable equipment and services. The increasing reliance of consumers, businesses and the government on broadband services is a testament to the industry's effective work in ensuring the reliability of traditional, transitional and next generation networks.

ATIS therefore believes that any Commission rules must "do no harm" to work underway in the industry to foster reliability and survivability. ATIS also believes that the Commission should collaborate with the industry in the development of standards and specifications aimed at fostering network reliability, rather than establishing regulatory mandates that may chill on-going industry work. Such cooperation with the industry is also necessary due to the complex and evolving nature of communications network; no regulation should impede the ability of service providers to offer new products and services to its customers or hamper the deployment of new and innovative technologies.

Among the ATIS industry forums that are producing work related to the deployment of reliable and robust broadband networks are:[1]

> **Copper/Optical Access, Synchronization and Transport (COAST) Committee**. COAST develops and recommends standards and technical reports for home, access and transport network and synchronization technologies over copper and optical mediums, including interfaces and functionalities that are required for access to, and transport through, telecommunications networks. The work includes the electrical, electromagnetic, optical, and mechanical characteristics of interfaces; the physical layer transmission and signaling protocols; hierarchical optical structures; network synchronization interfaces; and wired home networking transceivers.
>
> **Network Reliability Steering Committee (NRSC)**. The NRSC strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry. The NRSC addresses network reliability improvement opportunities in an open environment and advises the communications industry through the development of standards, technical requirements, technical reports, bulletins, Best Practices, and annual reports. The NRSC is comprised of industry experts with primary responsibility for examining, responding to and preventing outages for communications companies.
>
> **Next Generation Interconnection Interoperability Forum (NGIIF)**. NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. It develops operational procedures that involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.
>
> **Network Performance, Reliability and Quality of Service Committee (PRQC)** PRQC develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks. PRQC also identifies and defines performance and measurement parameters for the speed, accuracy, dependability, availability, and robustness of connection establishment/disengagement and information transfer, and develops transmission planning guidance for the deployment of signal processing devices such as echo cancellers and VoIP elements.

[1] More information about these committees is available from the ATIS website at: http://www.atis.org/committees/.

Packet Technologies and Systems Committee (PTSC). PTSC develops and recommends standards and technical reports related to packet services, architectures, and signaling, and related subjects, including next generation carrier interconnection, signaling architecture and control, and security.

Sustainability in Telecom: Energy and Protection Committee (STEP). STEP develops standards and technical reports in the areas of energy efficiency, environmental impacts, power and protection. The work of STEP enables vendors, operators and their customers to deploy and operate reliable, environmentally sustainable, energy efficient communications technologies.

Wireless Technologies and Systems Committee (WTSC). WTSC develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies.

II. Network Vulnerabilities

In the *NOI*, the Commission seeks information about the impact that one or more points of failure may have on broadband communications networks.[2]

As an initial matter, ATIS notes that service providers take reasonable and appropriate steps to mitigate network failures and have designed their networks to be robust and to provide reliable service to end users. As part of this effort, the ATIS NRSC has been working collaboratively with the Commission over the last 17 years to examine and mitigate potential vulnerabilities and enhance the reliability of communications networks. However, all communications networks have potential points of failure and, despite the best efforts of service providers, no system can be expected to be 100% reliable in all situations. ATIS therefore supports the Commission's efforts to gain a better understanding of the survivability of networks.

When discussing points of failure, it is important to consider the complex nature of communications systems and system architectures and deployment. Networks are

[2] ATIS notes that the Commission also seeks input on its legal authority to adopt specific measures to reduce broadband network vulnerabilities. *NOI* at ¶¶8-9. ATIS' comments do not address this issue.

comprised of many different technologies, both legacy and next generation, and each carrier may deploy its network differently to take into account factors such as consumer demand and use, available spectrum, topography and equipment availability. As such, potential single points of failure will vary by platform, technology and/or service provider.[3] For instance, a loss of a cell site may not be a single point of failure for a particular service provider if the loss occurs in an area where there is overlapping wireless coverage and is sufficient network capacity.

ATIS agrees with the FCC's assessment that "[b]roadband core networks are generally presumed to be quite survivable. Survivability is generally weaker in segments of communications networks closer to the network edge…"[4] Broadband networks are most vulnerable to single points of failure in the last mile from the customer premise to the network's edge. However, ATIS notes that failures in this part of the network affect fewer customers. ATIS also notes that the impact of a potential failure on the core of a broadband packet network will be significantly different than a similar failure on the legacy public switched telephone network. In the packet network core, there is greater resiliency and therefore a reduced likelihood that a failure would result in blocked service. Instead a failure may only result in a degradation of service (such as increased latency). Additionally, service providers have business continuity and disaster recovery plans to help ensure that service is normalized as soon as practical.

In the *NOI*, the Commission also asks what measures communications providers

[3] ATIS notes that the FCC references VoIP servers as an example of a failure in a broadband architecture. *NOI* at ¶10. However, it is important to note that VoIP is a service and not an architecture.
[4] *NOI* at ¶7.

take to minimize the presence of single points of failure in broadband architectures.[5] ATIS notes that service providers utilize geographic and component redundancy in their networks. Service providers are also active participants in standards development organizations and industry forums to develop network capabilities and Best Practices to promote resiliency. Finally, ATIS notes that service providers also maximize physical and equipment diversity where possible.

However, despite the diligent efforts of service providers, there are circumstances that may result in a loss of service. Obviously, manmade and natural disasters can affect the network or can increase network traffic beyond engineered capacity. Networks cannot be designed or implemented to withstand every possible source of failure. In addition, there are technical limitations that may restrict what service providers can do. For instance, in the last mile, it may be difficult to deploy diverse equipment due to factors such as geography, rights of way, licensing territories, and physical availability. Finally, it is important to note that service providers' efforts reflect a variety of considerations, including the needs of customers, engineering practices, etc.

Service providers take steps to measure and understand the impact of outages on their customers. One way they do this is by deploying alarms as appropriate to monitor their broadband networks. Service providers also hold routine operational reviews to evaluate Key Performance Indicators (KPI) and measure key aspects of the network (e.g., failure scenarios, traffic routing, single points of failure, fault and performance, etc.). Finally, ATIS notes that service providers have audit and review processes that address general diversity and track the diversity of critical circuit types such as 911, airports, and

[5] *NOI* at ¶10.

other lifeline services as appropriate.

Service providers also take steps to foster the reliability and availability of communications used by public safety agencies. For instance, service providers provide technical and operational support to public safety answering points (PSAPs) to support the PSAPs' own operational plans for diversity and redundancy.[6] As well, carriers encourage first responders to apply for Telecommunications Service Priority (TSP) authorization codes.[7] Under the rules of the TSP system, telecommunications services vendors are both authorized and required, when necessary, to provision and restore those telecommunications services with TSP assignments before services without such assignments. Additionally, service vendors are allowed to preempt non-TSP customer services in order to restore TSP coded services.

In the *NOI*, the Commission asks whether broadband traffic critical to response agencies or for critical services should be prioritized.[8] ATIS notes that substantial industry work is underway to develop technical standards/protocols that would permit such prioritization.[9] However, these standards are not yet finalized. ATIS urges the Commission to work closely with the industry before looking to adopt regulations regarding this issue and to look to existing priority communications programs (e.g.,

[6] It is important to note that it is the responsibility of the PSAPs to build diversity/redundancy into their own operational plans. Service providers can only provide advice and support and cannot control PSAP operational plans.

[7] In the *NOI*, the Commission asks about the survivability of cell sites used by first responders. *NOI* at ¶10. ATIS notes that it is not possible to associate specific cell sites with first responders. However, service providers engineer the highest level of survivability into cell sites consistent with business and customer usage patterns (e.g. hardware and fiber redundancy).

[8] *NOI* at ¶10.

[9] For instance, the ATIS PTSC is developing standards that address prioritization, including Emergency Telecommunications Service (ETS) Wireline Access Requirements (Issue S0081), ETS Phase 2 Network Element Requirements (Issue S0082), and NGN GETS (ETS) End-to-End Call Flows (Issue S0085). ATIS understands that similar work is underway in other organizations such as the Internet Engineering Task Force as well as in the 3rd Generation Partnership Project, in which ATIS is an organizational partner.

Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS)) as models for broadband prioritization).

The Commission also asks whether there could be dual failures that could impact a large number of users for an extended period of time. ATIS notes such dual failures could arise, particularly in situations such as natural disasters. Extraordinary events, such as earthquakes, floods, or asteroid strikes, could destroy a large enough area to impair any designed physical diversity. Dual failures could also arise during large scale commercial power outages that affect multiple nodes. Other examples of dual failures that could impact large numbers of customers would be multiple fiber cuts (i.e., cuts in 2 or more separate areas), which could isolate parts of networks, or one or more fiber cuts that occur simultaneously with a device failure, which could disrupt a portion of the network. However, it should be noted that the probability of these events happening is extremely small.

III. Industry Best Practices

A second major area on which the Commission seeks comment in the *NOI* is on the survivability of physical facilities in which network elements are located, including the relevant Best Practices used by the industry.

ATIS notes that Best Practices are extremely important to the industry. The primary objective of Best Practices is to provide guidance based on industry expertise and experience. The success of these Best Practices in enhancing network reliability stems from their development in a voluntary and consensus-based environment that encourages a pooling of expertise that is used to both identify and thoroughly examine potential Best

Practices.[10] ATIS strongly believes that the Commission must not disrupt this environment by imposing unnecessary regulatory mandates on the use of Best Practices. Adherence to Best Practices therefore must remain voluntary and the decision whether or not to implement a specific Best Practice should be left to individual providers. The voluntary nature of Best Practices was perhaps best described in the Final Report of the NRIC VII Focus Group 2A (December 2005):

> Mandated implementation of these Best Practices is not consistent with their intent. The appropriate application of these Best Practices can only be done by individuals with sufficient competence to understand them. Although the Best Practices are written to be easily understood, their meaning is often not apparent to those lacking experience and/or expertise in the specific job functions related to the practice. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations' regarding intended use, the industry is concerned that government authorities may inappropriately impose these as regulations or court orders.

Best practices, including NRIC physical security Best Practices, are widely deployed by the industry as applicable. For instance, service providers have implemented Best Practices related to access control devices, security policies and procedures,[11] security controls (including video surveillance systems, security officers, alarms and hardening of physical plant),[12] and pre-employment background screening of employees.[13]

Individual service providers typically develop their own internal physical security standards and policies, which incorporate applicable elements of the NRIC Best Practices. NRIC physical security Best Practices, along with emerging security methods and

[10] Many industry Best Practices are developed in industry organizations such as ATIS. The ATIS NRSC develops Best Practices related to the reliability of communications networks and generally presents these Best Practices for adoption to the Network Reliability and Interoperability Council (now the Communications Security, Reliability and Interoperability Council).

[11] *See* BPs 7-7-8086, 7-7-0814, 7-6-5023.

[12] *See e.g.,* BPs 7-7-0649, 7-7-5011.

[13] *See e.g.,* BPs 7-7-5033, 7-7-5034, 7-7-8099.

technologies, are routinely evaluated by providers' security subject matter experts for relevance and implementation. Further, providers also conduct risk assessments of key facilities to ensure adequacy of physical security relative to potential threats and the consequence of failure.

While NRIC physical security Best Practices have been widely adopted and implemented, there are situations in which a best practice may not be implemented by a service provider. Such decisions are made based on the aforementioned subject matter expert evaluations, risk assessments, and/or other considerations. In some situations, a best practice may have been superseded by provider-specific internal practice(s). It is important to note that all service providers have their customers' needs and the protection of the network as primary concerns. Therefore, service providers constantly strive to ensure the highest level of network protection practicable.

IV. Redundancy

A third topic on which the Commission seeks input in the *NOI* concerns the level of redundancy in broadband communications network and the Commission's role in increasing this redundancy.

As part of their efforts to provide reliable networks, service providers employ physical diversity and redundancy in their networks. Before equipment is deployed, a detailed evaluation and site survey process is undertaken that includes a review of transport facility availability and diversity. The decision regarding how and where to deploy equipment is based on a myriad of factors, including the service provider's engineering practices, standards and the needs of customers or tiers of customers.

Despite the deployment of redundant systems, ATIS notes there may be instances under which there could be a failure of all available paths; however, this would be extremely rare and likely be the result of a cataclysmic event. The distributed nature of broadband networks means that these networks may be vulnerable to equipment failures or data corruption (i.e. improper configuration/operation) causing localized outages.

In the *NOI*, the Commission also asks to what extent switching and routing capacity in broadband communications networks is protected by redundant systems or reserve switching capacity.[14] ATIS notes that such protections are indeed employed. Their use is based on established engineering practices and the availability of reserve switching capacity and bandwidth. It is important to note that the availability of reserve switching capacity and bandwidth are consumer-driven characteristics. Individual service providers may have different capacities based on their own consumers' traffic patterns and estimates of future growth.

V. Severe Overloads

The *NOI* also focuses on the impact that events such as natural disasters or pandemics could have on broadband networks.

ATIS notes that service providers routinely deal with severe weather events and have significant experience in mitigating the impacts of such events and in successfully restoring service.[15] Weather, such as snowstorms and weather-related natural disasters, have the single largest impact on broadband networks and can serve to increase peak-time

[14] *NOI* at ¶14.

[15] The ATIS NRSC has published a set of Pandemic Planning recommendations that includes a compilation of Best Practices to ensure service provision, and business continuity in the event of a pandemic outbreak. The Best Practices are available at: http://www.atis.org/nrsc/Docs/NRSC_Pandemic_Checklist_Final.pdf.

downstream traffic loads, create localized congestion or reduce throughput. However, internet “outages” or brownouts caused by overloads are rare events.

ATIS notes that the capacity of residential access networks is sufficient to handle sudden surges in use. Such capacity was put to the test in the recent events during the Northeast snowstorms of 2009-2010. During these events, there was sufficient capacity on residential broadband networks to successfully handle the significant increase in telework activity and associated increased traffic.

While residential broadband networks are engineered to meet peak busy hour traffic demands, these networks cannot be designed to have sufficient spare capacity in all possible situations. Sustained, unexpected traffic from the entire service population would result in congestion and lowered average throughput speeds for customers. Unexpected traffic loads during peak times could also result in congestion and lower throughput speeds.

In the event of congestion, service providers have a range of network management solutions. In many cases, the impact of these management tools will be imperceptible to individual users and these users will not experience service impacts. In situations involving more severe congestion, however, end users may notice some degradation in service. In determining which solution to implement in a given situation, service providers balance the impact to customers with the need to preserve and protect their networks.

Broadband networks are designed to allow providers to maintain control and dynamically react to congestion or outages. For instance, to ensure access to network equipment, the control plane data associated with broadband networks, which is necessary to correctly route data, is either prioritized or carried on a separate network. Intelligence is also built into the network to ensure the network can dynamically react to certain capacity constraining events. An example of this is “Auto-Bandwidth,” which allows a Multiprotocol Label Switching enabled network to react to congestion by routing traffic to parts of the network where bandwidth is available, rather than strictly following “shortest-path” routing protocol heuristics.

ATIS notes that some broadband congestion is self-correcting given that many applications use Transmission Control Protocol (TCP), a protocol that will self-level the throughput of a given stream based on latency and packet loss. For short term congestion, the prevalence of TCP-based applications means that congestion may slow the operation of broadband applications but will not likely prevent their operation. Additionally, certain high-bandwidth applications (such as online gaming, VoIP, video-conferencing, Virtual Private Networks, and remote desktop connections) often have minimum baselines to be viable; during times of severe congestion, the necessary latency/throughput baselines may not be available and these high-bandwidth applications may not operate, further reducing congestion.

VI. Commission Role

Finally, the Commission asks in the *NOI* for input on what its role should be in reducing points of failure, promoting Best Practices and enhancing diversity and redundancy.

As noted above, while no network can be designed to be 100% reliable at all times and in all situations, the communications industry does a remarkable job in ensuring that US broadband networks are highly reliable. Individually and through organizations such as ATIS, the industry works to develop standards and Best Practices that maintain and enhance this reliability. ATIS therefore believes that the Commission should support and not supplant the industry efforts.

ATIS recommends that the Commission: (1) support and promote awareness of industry-developed standards and Best Practices; (2) continue to partner with industry forums such as the ATIS NRSC to identify issues around which the development of Best Practices would be beneficial; and (3) explicitly recognize and support the ability of industry to develop, implement and revise Best Practices according to their business needs and requirements.

VII. Conclusion

While broadband networks are reliable, ATIS notes that they cannot be designed to withstand every point of failure. Service providers work extensively to enhance reliability through a variety of means, including the implementation of Best Practices and the utilization of geographic and component redundancy in their networks. In the event of network congestion from sustained, unexpected traffic, service providers also have network management solutions available. The Commission also has a role in promoting network reliability by: (1) supporting and promoting awareness of industry-developed standards and Best Practices; (2) continuing to partner with industry forums to identify issues around which the development of Best Practices would be beneficial; and (3) explicitly recognizing and supporting the ability of industry to develop, implement and revise Best Practices according to business requirements.

Respectfully submitted,

Alliance for Telecommunications Industry Solutions
By:

Thomas Goode
General Counsel

Dated: June 25, 2010