Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Reliability and Continuity of Communications Networks, Including Broadband Technologies	)	PS Docket No. 11-60
	)	
Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload	)	PS Docket No. 10-92
	)	
Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)	EB Docket No. 06-119

COMMENTS OF
THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

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

July 7, 2011

TABLE OF CONTENTS

SUMMARY

In its comments, ATIS provides input on specific questions raised in the *NOI*. ATIS notes that there are general principles surrounding network resiliency that should be considered, namely that: communications networks are reliable and service providers are strongly incented to maintain and enhance this reliability; the Commission's goal should not be to mandate a redesign of the network, but to allow the industry to continue to effectively maintain and upgrade the network; there is no single set of Best Practices applicable to all circumstances; and networks cannot be designed or implemented to withstand every possible source of failure.

ATIS notes its appreciation for the Commission's ongoing dialogue with the industry and observes that such a dialogue is the most effective way to promote the development of Best Practices and to stimulate innovation. ATIS also strongly supports the Commission's efforts to seek information on the practical impact that regulatory mandates may have on network resiliency.

With regard to service continuity, ATIS notes that service providers have mature, comprehensive crisis management structures and business continuity plans for critical functions. ATIS believes that no additional actions are necessary by the Commission to ensure that the public continues to have access to communications during major emergencies.

ATIS also believes that there is no reason for specific backup power requirements or for other Commission mandates that dictate how service providers build reliable networks and restore service. Instead, it urges the Commission to take a holistic view of service continuity and recognize that many factors influence service providers' decisions regarding backup power. ATIS notes that service providers are also in the best position to determine how to restore service and explains that providers prioritize restoration efforts for: Telecommunications Service Priority customers; police, fire and 911 facilities; hospitals; and airports.

As to broadband reliability, ATIS observes that the implementation of IP-based systems has not resulted in the degradation of reliability or resiliency. Service providers still set stringent targets for system performance reliability and require equipment vendors to provide specific reliability metrics that permit the providers to make informed decisions. There is therefore no need to set downtime objectives or establish other reliability standards.

While ATIS acknowledges that planned maintenance activities can affect service, Best Practices are effectively used by the industry to mitigate procedural, process, or equipment failures during maintenance. ATIS strongly cautions against drawing conclusions pertaining to the impact of maintenance on network reliability or availability.

As it has in previous comments, ATIS notes that, to the extent that vulnerabilities exist in broadband networks, they are likely to be present the "last mile" from the network's edge to the customer premise. Such vulnerabilities likely affect fewer customers and are less likely to result in blocked service. ATIS also explains that providers have safeguards in place to mitigate vulnerability to cascading overloads and to prevent silent failures.

Finally, ATIS recommends that the Commission: (1) complete its work to redesign the Universal Service Fund so that funds can be made available for the building of robust networks; and (2) continue its collaboration with the industry within ATIS NRSC and elsewhere to promote the development and use of voluntary Best Practices relating to reliability and resiliency.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Reliability and Continuity of Communications Networks, Including Broadband Technologies	)	PS Docket No. 11-60
	)	
Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload	)	PS Docket No. 10-92
	)	
Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)	EB Docket No. 06-119

COMMENTS
OF THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

The Alliance for Telecommunications Industry Solutions (ATIS) on behalf of its Network Reliability Steering Committee (NRSC), hereby submits these comments in response to the Commissions' *Notice of Inquiry* (*NOI*) in the above-referenced dockets. ATIS' comments reflect input from subject matter experts on selected topics raised in the *NOI*. In general, and as explained more fully below, ATIS supports the Commission's efforts to gain a better understanding of the industry efforts to promote resilience and reliability. However, because service providers are already strongly incented to provide reliable service and have designed their networks to be resilient and robust, ATIS does not believe new rules regarding this matter are needed. Instead, ATIS urges the Commission to continue to afford the industry the flexibility to effectively maintain and upgrade this infrastructure to meet new challenges.

I. BACKGROUND

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. ATIS' diverse membership includes key stakeholders from the information and communications technologies industry –wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, digital rights management companies, and internet service providers. Nearly 600 industry subject matter experts work collaboratively in ATIS' open industry committees.

Formed in 1993 at the recommendation of the first Network Reliability and Interoperability Council, the ATIS 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, reports, bulletins, Best Practices, and annual reports. The NRSC is comprised of industry experts with primary responsibility for examining, responding to, and preventing service disruptions for communications companies. NRSC participants are the industry subject matter experts on communications network reliability and outage reporting.

The ATIS NRSC is only one of ATIS' committees with work programs directed at facilitating the reliability and resiliency of networks. Other ATIS Committees with relevant work programs include: Copper/Optical Access, Synchronization and Transport Committee; Next Generation Interconnection Interoperability Forum; Network Performance, Reliability and Quality of Service Committee; Packet Technologies and Systems Committee; Sustainability in Telecom: Energy and Protection Committee; and Wireless Technologies and Systems Committee.

II. GENERAL COMMENTS

In the *NOI*, the Commission takes yet another look at the reliability of communications networks and the ability of service providers to meet the critical needs of their customers. The Commission acknowledges that this proceeding raises issues previously discussed in numerous recent *NOI*s and *Notices of Proposed Rulemaking*, but sees this proceeding as complimentary to, rather than redundant with, those proceedings.[1]

ATIS does not take issue with the Commission's revisiting of these matters in this *NOI*. The reliability and resiliency of communications networks is vitally important to this country and to all consumers. ATIS agrees that this matter should be a primary focus of the Commission, just as it has always been a primary focus of communications service providers and equipment providers. However, ATIS urges the Commission, in this and any future rulemakings, to acknowledge certain fundamental truths about networks and network reliability/resiliency. Many of these points have been made by ATIS and others previously, but they bear repeating:

- U.S. communications networks are reliable and service providers are strongly incented to maintain and enhance this reliability. The communications industry spends billions of dollars to improve the capabilities and reliability of their networks.[2] This effort is expended not because of a regulatory mandate, but because the marketplace demands it. There is little the Commission can or should do to provide more of an incentive than the marketplace already provides. In fact, as explained more fully below, ATIS believes that additional regulation may adversely affect the marketplace.
- The Commission's goal should not be to mandate a redesign of network infrastructure, but rather to allow the industry to continue to effectively maintain and upgrade this infrastructure. The U.S. communications network is not a single network, but an interconnected set of networks. Reliability and resiliency therefore depend on a complex set of factors and the industry, not the Commission, is in the best position to understand how to promote and provide the associated reliability. Mandating network configurations, technology, and processes in an attempt to create the "perfect" network will undermine progress and redirect or strand funding away from new technologies and toward the maintenance of a mandated *status quo*.
- There is no single set of Best Practices applicable to all circumstances. Not all service-impacting events are alike. While there may be ways of mitigating some service

[1] *NOI* at ¶¶7-13.

[2] For instance, the FCC recently noted that the industry invested $65 billion in capital expenditures in 2010 alone. *See* http://www.fcc.gov/reports/seventh-broadband-progress-report.

disruptions in certain circumstances, many types of disasters (earthquakes, floods, tornadoes) can cause such significant damage that there may simply be no cost-effective methods to meaningfully minimize or prevent the impact of these events.

- Networks cannot be designed or implemented to withstand every possible source of failure. While network reliability is a laudable goal, there is no way that networks can be 100% reliable in all circumstances.

ATIS strongly supports the approach taken by the Commission in this *NOI*, and in the separate but related *NPRM* regarding outage reporting, to seek information not simply on the abstract issue of network resiliency, but on the practical impact that any regulatory mandates may have on this resiliency.[3] By acknowledging and seeking information on the burdens associated with any new regulations, the Commission can avoid imposing new regulatory mandates that exacerbate the already significant burdens associated with communications outage reporting. As ATIS has previously noted, the Commission has not been entirely successful in judging the burdens associated with its outage reporting rules, substantially underestimating the total number of reports, associated submission times and costs.[4] ATIS urges the Commission to carefully consider all burdens before imposing any new regulatory mandates.

ATIS appreciates the Commission's interest in continuing its ongoing dialogue with the industry.[5] The Commission's informal dialogue with the industry through groups such as the ATIS NRSC is the most effective way to promote the development of Best Practices and to stimulate "out of the box" thinking and innovation. ATIS notes that the industry has a proven record of innovation in areas pertaining to service continuity and resiliency. Such innovation is a necessary component to service continuity because it allows the industry to proactively address

[3] The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, PS Docket No. 11-82, *Notice of Proposed Rulemaking* (rel. May 13, 2011) (*Broadband Outage Reporting NPRM*).

[4] *See* ATIS' Comments in response to the Commission's 2010 Biennial Review of Regulations Administered by the Public Safety and Homeland Security Bureau, PS Docket No. 10-270, *Public Notice* (rel. December 20, 2010). ATIS concerns have proven well-founded. For instance, when the Commission's outage reporting rules were adopted, the number of filings was estimated to be significantly less than 1,000 per year. Recently, the Commission noted the actual number of filings is closer to 11,000 per year. *Broadband Outage Reporting NPRM*, Appendix B, ¶42.

[5] *NOI* at ¶6.

the challenges associated with new technologies and with the continued evolution of the network. Regulatory mandates cannot be as effective as industry efforts, and may instead adversely affect the pace of innovation, increase costs and create rigidity into what would have been an otherwise flexible process.

III. CONTINUITY OF SERVICE

A significant portion of the *NOI* concerns the ability of communications networks to provide continuity of service during major emergencies, such as large-scale natural and man-made disasters.[6] As stated above, ATIS strongly believes that U.S. communications networks are reliable and that providers are incented to take appropriate steps to protect their networks against failures and to restore service caused by major emergencies.

ATIS notes that service providers have highly matured comprehensive crisis management structures and business continuity plans for critical functions at locations throughout the U.S. and internationally. These plans, which are cross-functional and involve the participation of different departments, are designed to ensure that providers can continue delivering services to their customers in the event of a significant natural or man-made event. Moreover, some companies use business continuity and disaster response checklists tailored to specific disasters (such as hurricanes, tornados, earthquakes and wildfires).

There are also broader industry efforts aimed at business and operation continuity and disaster recovery. ATIS NRSC has developed checklists pertaining to specific events, such as hurricanes and pandemics, that can help to mitigate against communications outages and facilitate the restoration of service.[7] In addition, CTIA – The Wireless Association™ has established a Business Continuity/Disaster Recovery certification program under which wireless

[6] *NOI* at ¶¶15-26.

[7] *See* ATIS NRSC Pandemic Checklist, Version 1 (ATIS-0100018), NRSC Hurricane Checklist (ATIS-0100019). These documents are available for free from the ATIS NRSC website at: http://www.atis.org/nrsc.

network operators can demonstrate that they have designed and implemented strategies to prevent and respond to network damage resulting from emergencies. This industry program, like the ATIS checklists, accommodates individual risk assessment and decision making that must be done by each service provider based on the technical and operational needs of its network.

The Commission also seeks information regarding industry Best Practices regarding the provision of service during major emergencies.[8] ATIS notes that there are many Best Practices that have been developed by the industry to address this issue and that these Best Practices are effective in promoting reliable communications during major emergencies. Given the sheer number of Best Practices and the fact that many of these practices address this issue either directly or indirectly, an exhaustive list would be difficult to compile. However, below are some of the more relevant industry Best Practices.

- 7-5-0514 When available, Network Operators and Service Providers should utilize a management system capability (e.g., CORBA, SNMP) providing a single interface with access to alarms and monitoring information from all critical network elements.
- 7-7-0406 Spares and Inventory: Network Operators and Service Providers should, where appropriate, establish a process to ensure that spares inventory is kept current to at least a minimum acceptable release (e.g., hardware, firmware or software version).
- 7-7-0504 Network Operators and Service Providers, in order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, should consider maintaining hot spares (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements.
- 7-7-0548 Post Mortem Review: Network Operators and Service Providers should have an internal post mortem process to complete root cause analysis of major network events with follow-up implementation of corrective and preventive actions to minimize the probability of recurrence. Network Operators and Service Providers should engage Equipment Suppliers and other involved parties, as appropriate, to assist in the analysis and implementation of corrective measures.
- 7-7-0552 Equipment Suppliers' software fault insertion testing (including simulating network faults such as massive failures) should be performed as a standard part of an Equipment Supplier's development process.
- 7-7-0553 Equipment Suppliers hardware fault insertion testing (including simulating network faults such as massive failures) should be performed as a standard part of an

[8] *NOI* at ¶21.

Equipment Supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress fault recovery software.

- 7-7-0566 Network Operators and Service Providers should consider placing and maintaining 911 circuits over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof).
- 7-7-0594 Maintaining SS7 Link Diversity: Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity. SS7 link diversification validation should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity.
- 7-7-0602 Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).
- 7-7-0612 Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.
- 7-7-0690 Network Operators and Property Managers should consider providing power alarm redundancy so that no single point alarm system failure will lead to a network power outage.
- 7-7-0697 Network Operators, Service Providers and Equipment Suppliers should employ an Ask Yourself program as part of core training and daily operations.
- 7-7-0726 Network Operators should consider partnering with excavators, locators, and municipalities in a cable damage prevention program.
- 7-7-0731 Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis.
- 7-7-0740 - Network Operators should implement internal processes needed to support the One-Call Notification legislation.
- 7-7-0758 Network Operators and Service Providers should, upon restoration of service in the case of an outage where 911 call completion is affected, make multiple test calls to the affected PSAP(s) to ensure proper completion.
- 7-7-5078 Network Operators and Service Providers should be automatically notified upon the loss of alarm data and react accordingly.
- 7-7-5083 Network Operators, Service Providers and Equipment Suppliers should maintain the availability of spares for critical network systems.
- 7-7-5237 Network Operators, Service Providers and Equipment Suppliers should verify the integrity of system spares and replenish utilized spares, as appropriate, as part of a disaster response at a facility.
- 7-7-5241 Network Operators, Service Providers and Equipment Suppliers should consider placing access and facility alarm points to critical or sensitive areas on backup power.

ATIS notes that 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 vast expertise and considerable resources. Best Practices provide guidance from assembled industry expertise and experience; such guidance cannot be easily duplicated on an individual company basis. However, as ATIS NRSC explained in its tutorial to the Commission's Communications Security, Reliability and Interoperability Council (CSRIC), Best Practices are more than just good ideas. They are practices which address recurring, or potentially recurring, challenges that have been proven through actual implementation, have been developed through rigorous deliberation and expert consensus, and have been confirmed by a broad set of stakeholders.[9]

ATIS further notes that Best Practices cannot be assumed to be applicable to all circumstances and therefore cannot be mandated. The Commission's CSRIC agreed that it would be impractical, if not impossible, to mandate compliance with Best Practices because not every Best Practice is appropriate for every sector of the industry, particularly as network and system designs, technologies, and capabilities differ and are evolving. CSRIC also noted that, even within a particular sector, not every practice is appropriate for every provider because the providers' have a different scope of activities, resources, and capabilities. The resource burdens of implementing certain Best Practices may be significant and CSRIC noted that these burdens should be considered by providers in determining which practices to implement.[10]

ATIS also observes that the voluntary nature of Best Practices encourage individual service providers to develop and incorporate internal standards and policies based on the Best Practices elements that are applicable, even when other elements may not be. Many large

[9] *See* November 10, 2010, Letter from Jackie Voss, ATIS Manager, to John Healy, Associate Chief of the Communications Systems Analysis Division of the Public Safety and Homeland Security Division, enclosing *NRSC Best Practices Tutorial* (November 2010).

[10] *Final Report of CSRIC Working Group 6: Best Practice Implementation* (January 2011), Recommendation 5.2. It is important to note also that providers may also decide not to implement a specific Best Practice based on internal evaluations, risk assessments, and/or other considerations (such as whether a specific Best Practice has been superseded by a provider-specific internal practice).

service providers publish their own technical documentation that are grounded in industry Best Practices, standards documents, and vendor documents to further enhance the reliability of their networks. In addition, organizations such as Telcordia Technologies develop industry requirement documents, which when utilized, enhances overall network reliability.

The Commission also seeks information on what actions, if any, it should take to ensure that the public continues to have access to communications during major emergencies.[11] ATIS does not believe that any additional actions are necessary by the Commission. Service providers take their responsibilities to provide reliable communications services to their customers very seriously and the maintenance and restoration of service is their primary concern. Regulatory mandates are not necessary. Instead, ATIS urges the Commission to continue to work with industry groups such as the NRSC and to endorse the use and continued development of industry-developed Best Practices.

The Commission correctly notes that one issue that has impacted the ability of service providers to restore service has been a lack of access to service provider sites located within disaster areas.[12] ATIS agrees the lack of access has hampered restoration efforts in the past, including those efforts to restore service after hurricanes, including Hurricane Katrina. ATIS also agrees with the Commission that steps have been taken to address this issue, but notes that access to sites after natural disasters remains a concern for the industry.

IV. BACKUP POWER

The Commission seeks comment in the *NOI* on how various backup power techniques or performance standards could or should be employed to ensure adequate levels of service continuity during major emergencies.[13] While ATIS agrees that the availability and reliability of

[11] *NOI* at ¶17.

[12] *NOI* at ¶18.

[13] *NOI* at ¶¶23-25.

backup power is one element that should be considered as part of an examination of service continuity, it is not the only one. In some cases, in fact, the availability of backup power may not be a primary element, especially if other parts of the network are damaged by floods, tornadoes, fires or earthquakes. In those cases, the existence of backup power may be irrelevant or premature to restoration efforts as service providers must focus on rebuilding or replacing other infrastructure, such as damaged equipment, towers and cables.

ATIS therefore believes that there is no reason for specific backup power requirements or for other Commission mandates that dictate how service providers build reliable networks and restore service. Instead, the Commission should take a holistic view of service continuity and recognize that many factors influence service providers' decisions regarding backup power. Among these factors are the geographic location of the site, site-specific space and weight constraints, and the technical needs of the network.[14] ATIS believes that service providers, not the Commission, are in the best position to evaluate these factors and make decisions regarding backup power.

Similarly, service providers are also in the best position to determine how to restore service. As noted above, service providers have continuity and emergency response plans in place. The providers prioritize efforts to restore service to critical operations first. Thus, efforts are undertaken to focus efforts first on: Telecommunications Service Priority (TSP) customers; police, fire and 911 facilities; hospitals; and airports (flight-affecting circuits). However, it should be noted that the dynamics of an event (e.g., can restoration efforts safely begin in a particular area?), its impact to the network (e.g., what infrastructure has been damaged?) and its impact on customer facilities (e.g., have these facilities been damaged or evacuated?) must also be considered in making restoration decisions. Service providers also coordinate with public

[14] ATIS notes that additional backup power generally requires more space. In many cases, it may not be physically possible to upgrade a site given existing space and weight limitations.

safety and emergency response personnel regarding service prioritization needs. These factors may impact decisions regarding which facilities can and should be restored first.

Another issue on which comments are sought in the *NOI* is what developments there have been in back-up power technology, including lower power consumption.[15] ATIS notes that the industry is actively examining new battery technologies and fuel sources, such as fuel cell technologies, wind power, and solar. Although these alternatives have not yet proven the necessary level of reliability needed for communication systems, any Commission mandates could interfere with these industry efforts to investigate and, where appropriate, to deploy new sources of backup power. Therefore, ATIS recommends that the Commission continue to support the industry's efforts to investigate new technologies, and refrain from mandating the use or development of any specific technology.

ATIS also notes that the industry has been working to examine ways to reduce power consumption by information and communications technology (ICT) equipment and has made significant progress pertaining to the development of industry standards on ICT power consumption. For instance, ATIS's Sustainability in Telecom: Energy and Protection Committee has published a series of standards related to the Telecommunications Energy Efficiency Ratio ("TEER"), which helps define the overall efficiency of a piece of equipment by quantifying its ratio of work performed to energy consumed.[16] These standards facilitate the ability of service providers to compare the energy efficiency of equipment offered by different vendors.

---

[15] *NOI* at ¶24.

[16] *See* Energy Efficiency for Telecommunication Equipment: Methodology for Measurement and Reporting – General Requirements Document (ATIS-0600015.2009); Energy Efficiency for Telecommunication Equipment: Methodology for Measurement and Reporting – Server Requirements Document (ATIS-0600015.01.2009); Energy Efficiency for Telecommunication Equipment: Methodology for Measurement and Reporting – Transport Requirements (ATIS-0600015.02.2009); and Energy Efficiency for Telecommunication Equipment: Methodology for Measurement and Reporting DC Power Plant – Rectifier Requirements (ATIS-0600015.04.2010); Energy Efficiency for Telecommunication Equipment: Methodology for Measurement and Reporting Facility Energy Efficiency (ATIS-0600015.05); and Energy Efficiency for Telecommunications Equipment: Methodology for Measurement and Reporting for Router and Ethernet Switch Products (ATIS-0600015.03.2009) These documents are available from the ATIS Document Center at: http://www.atis.org/docstore.

V. RELIABILITY AND RESILIENCY OF BROADBAND NETWORKS

The second part of the *NOI* focuses on ways in which the Commission can bolster the reliability of U.S. broadband communications networks.[17] ATIS notes that the reliability of the broadband network was addressed by the industry in response to the Commission's April 2010 *Broadband Resiliency NOI*. In that inquiry, the Commission stated that "[b]roadband core networks are generally presumed to be quite survivable."[18] In its comments to the *Broadband Resiliency NOI,* ATIS agreed and further recommended against unnecessary regulatory mandates in this area given the effectiveness of service providers in providing reliable broadband services.[19]

It is important to understand that the implementation of IP-based systems has not resulted in the degradation of reliability or resiliency. While equipment and technologies have changed, the reliability requirements imposed by providers for the deployment and operation of this equipment and technology have not. Service providers still set stringent targets for system performance reliability and demand from their vendors that equipment is tested to ensure that it is sufficiently robust. Examples of this resiliency can be seen in the ability of service providers to offer reliable service even during significant storms and other events. The northeast snowstorms of 2009-2010 are one such example. Despite record amounts of snowfall, the broadband networks remained reliable and were able to successfully handle the significant amount of increased traffic and the residential utilization shift associated with remote work (i.e., telework).

The transition to IP-based systems has in fact <u>increased</u> overall resiliency. Broadband networks are designed to allow providers to maintain control and dynamically react to

[17] *NOI* at ¶28.

[18] *Broadband Resiliency NOI* at ¶7

[19] ATIS Comments to *Broadband Resiliency NOI* at p 3.

congestion and/or failures. "Auto-Bandwidth," for example, allows a Multiprotocol Label Switching (MPLS) enabled network to react to congestion by routing traffic to parts of the network where bandwidth is available. Broadband networks can also "self-correct" for congestion via the use of Transmission Control Protocol (TCP), which will self-level the throughput of a given stream based on latency and packet loss.

The Commission, in the *NOI*, asks about retransmission and rerouting techniques used to address network hardware resiliency and why some broadband transport protocols do not take full advantage of these techniques.[20] While it may seem that such rerouting and retransmission would be beneficial, ATIS notes that in some circumstances the retransmission of data following a loss is not desirable. A conversation over VoIP, for example, would be degraded and not enhanced if a packet previously dropped were retransmitted and arrived out of order.

ATIS appreciates efforts that have been undertaken to remove unnecessary restrictions and streamline processes that permit the deployment of broadband infrastructure. One such example is the Commission's *Shot Clock Ruling*, which addressed the timeliness of state and local permitting processes for tower siting applications and defines what is presumptively a "reasonable time" beyond which inaction on a siting application constitutes a failure to act.[21] ATIS believes that additional opportunities may be available to further streamline wireless broadband deployment, including those related to wireless siting, and notes that the Commission has issued an *NOI* on this matter.[22]

[20] *NOI* at ¶29.

[21] Petition for Declaratory Ruling to Clarify Provisions of Section 332(c)(7)(B) to Ensure Timely Siting Review and to Preempt Under Section 253 State and Local Ordinances that Classify All Wireless Siting Proposals as Requiring a Variance, WT Docket No. 08-165, *Declaratory Ruling*, 24 FCC Rcd 13994 (2009).

[22] *Acceleration of Broadband Deployment: Expanding the Reach and reducing the Cost of Broadband Deployment by Improving Policies Regarding public Rights of Way and Wireless Facilities Siting*, WC Docket No. 11-59, Notice of Inquiry (rel. April 7, 2011).

A. Equipment Downtime, Redundancy

The Commission also asks whether manufacturers provide adequate estimates of relevant reliability data for major pieces of equipment that they develop and about the typical downtime objective of core broadband devices.[23] ATIS notes that most service providers require equipment vendors to provide specific reliability metrics, for example, mean time between failure (MTBF), based on a Generic Requirements document created by Telcordia Technologies.[24] This information is sufficient to allow service providers to make informed decisions about equipment and its likely impact on the reliability of the network. However, ATIS strongly cautions against the Commission setting downtime objectives or other reliability standards, noting that there is no evidence that the application of standards to specific pieces of hardware would improve the overall operation of the service in a redundant carrier network.

ATIS similarly recommends that the Commission not set overall service goals for redundancy in the network. Methods for gauging reliability should be based on service availability rather than the availability of a specific piece of equipment. Each service provider should have the discretion to gauge the importance of a given service and provide an adequate level of redundancy and service availability. After all, service providers have a proven track record of keeping critical services (i.e. root DNS servers) operating under duress even without regulation.

The Commission also asks about the use of MPLS to facilitate the creation of "virtual links" between distant nodes as a way to ensure Quality of Service (QoS) for broadband services.[25] ATIS notes that MPLS and its associated link and node protection schemes make

[23] *NOI* at ¶¶30-31.

[24] Generic Requirements for Assuring the Reliability of Components Used in Telecommunications Equipment, GR-357.

[25] *NOI* at ¶33.

broadband service more resilient to failures by allowing service providers to recover more quickly from a link or node failure. As a result, MPLS dramatically increases the end-to-end availability of the network.

B. Capacity Issues

The Commission seeks comment in the *NOI* on system capacity issues, including whether capacity differs between public switched telephone network (PSTN) infrastructure and IP technology, with respect to redundancy, recovery and other relevant factors.[26]

As ATIS has explained in other proceedings, capacity has not generally been an issue in broadband networks. In fact, the capacity of broadband access networks is generally sufficient to handle both routine traffic and sudden surges in use.[27] While there are situations in which sustained, unexpected traffic from the entire service population could result in congestion and lowered average throughput speeds, ATIS strongly believes that service providers, not the Commission, must make decisions regarding where and when to add capacity. Mandated over-engineering to needlessly expand capacity would inhibit future growth and slow the evolution of the PSTN to an all IP-based network. Such over-engineering would also increase the costs of deploying broadband systems – costs that would be born not just by service providers but also by their customers. As noted above, the Commission's goal should not be to mandate a redesign of network infrastructure, but rather to allow the industry to continue to effectively maintain and upgrade this infrastructure.

[26] *NOI* at ¶37.

[27] ATIS' Comments to Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, *Notice of Inquiry* (rel. April 21, 2010) at p.12.

C. Cascading Overloads & Graceful System Recovery

Another issue on which the Commission seeks input concerns how to ensure graceful system recovery and mitigate vulnerability to cascading failures.[28] ATIS notes that service providers have equipment safeguards and practices in place to both mitigate vulnerability to, and to ensure a graceful recovery from, cascading overloads. One way in which the risks of such overloads are minimized is by localizing systems and removing unnecessary remote dependencies (e.g., proper design, sizing, segmentation). Another way is to ensure that the equipment purchased from vendors is engineered to perform satisfactorily when, for example, recovering from a power failure or authenticating large volumes of users simultaneously. The prevention of and recovery from such overloads can best be viewed as a joint effort by service providers, who are responsible for management of the network, and equipment vendors, who are responsible for the provision of appropriately engineered and tested equipment.

The Commission also asks about the need for additional capacity of back-up paths to meet the needs of users or equipment trying to reestablish service.[29] ATIS does not believe that there has been a significant reliability or resiliency issue pertaining to the capacity of these backup paths. ATIS therefore recommends that decisions regarding the establishment of these paths should be left to service providers, who can best evaluate the need for additional capacity.

D. Maintenance Procedures

The Commission notes that planned maintenance contributes to network failures and seeks information pertaining to safeguards currently in place to minimize disruptions caused by maintenance activities.[30] The Commission further notes that it has been reported that 20 percent

[28] *NOI* at ¶38.

[29] *Id.*

[30] NOI at ¶39.

of all failures on broadband networks may be due to planned maintenance.[31] While ATIS agrees that planned maintenance activities can affect service, it strongly cautions against drawing conclusions pertaining to the impact of maintenance on network reliability or availability based on an estimate from a 2004 study of a single service provider's network.

ATIS also notes that there are Best Practices used to mitigate procedural, process, or equipment failures during maintenance. For instance, service providers generally try to schedule maintenance after peak hours to minimize customer impact and to better allow the network to absorb rerouting traffic. These Best Practices also include the implementation of change management systems and Methods of Procedure (MOP) to evaluate maintenance work for technical correctness, avoid conflicting/overlapping maintenance activities and minimize the impact of these activities. Use of MOPs also allow service providers to accomplish work via established procedures that have been proven effective. Finally, it should be noted that providers verify the state of the network prior to and after maintenance occurs to verify the proper operation of their networks.

Specific industry Best Practices relevant to planned maintenance include, but are not limited to, the following:

- 7-5-0536 As appropriate, Network Operators and Service Providers should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Prior to deployment, appropriate testing should be conducted to ensure that such software updates are ready for deployment in live networks. Equipment Suppliers should include such software updates in the next generic release and relevant previous generic releases.
- 7-6-8037 System Inventory Maintenance: Network Operators and Service Providers should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.
- 7-7-0413 Maintenance Notification: Network Operators and Service Providers should communicate information on service affecting maintenance activities and events to their customers, as appropriate.

[31] *Id*. citing *Characterization of Failures in an IP Backbone*, Athina Markopoulou (Stanford University), Gianluca Iannaccone (Intel Research), Supratik Bhattacharyya (Sprint ATL), Chen-Nee Chuah (UC Davis), and Christophe Diot (Intel Research) (IEEE Infocom 2004).

- 7-7-0414 Maintenance Notification: Network Operators and Service Providers should establish plans for internal communications regarding maintenance activities and events that impact customers.
- 7-7-0418 Back-out MOPs: Network Operators and Service Providers should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.
- 7-7-0595 Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.

ATIS urges the Commission to allow the industry to continue to analyze and take any appropriate actions to address issues pertaining to planned maintenance.

E. Single Points of Failure

The Commission also seeks comment relating to the existence of single points of failure in broadband networks.[32] As ATIS has said previously, no network can be designed to be 100% reliable in all circumstances, nor would it be cost-effective to try to do so.

While broadband networks are generally very reliable, to the extent that vulnerabilities do exist in these networks, they are likely to be present the "last mile" from the network's edge to the customer premise. However, single points of failure in this area of the network: (1) will likely affect fewer customers; and (2) be less likely to result in blocked service. ATIS also notes that there are inherent levels of redundancy (such as link redundancy) in broadband networks. Industry practices that decrease the likelihood of an edge device becoming a single point of failure have been developed, and are currently in use. The practices include:

- a standardized software environment to ensure that issues are well understood and can be consistently worked;
- restrictions on access to information to reduce the possibility of human error in data collection;
- the creation of a standardized configuration template to prevent misconfigurations;

[32] *NOI* at ¶40.

- use of automated information gathering methods to facilitate the expeditious and proactive resolution of issues;
- requirements that device turn-up for IP DSL Gateways and aggregation devices be performed by appropriately trained personnel;
- ensuring that sufficient capacity is in place so that failure of a redundant link will not result in saturation of the remaining circuit; and
- implementation of a standardized network architecture to ensure that sites with comparatively little traffic receive the same level of service as the largest metropolitan area.

In addition to these practices, as noted above, service providers also have business continuity and disaster recovery plans to help ensure that service is normalized as soon as practical. Service providers also utilize geographic and component redundancy in their networks to minimize the impact of single points of failure and deploy alarms to monitor the impact of failures on their networks.

Other relevant Best Practices include:

- 7-7-0814 For the deployment of Residential Internet Access Service, Broadband Network Operators should design in the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance, security, or usage policy.
- 7-7-0817 For the deployment of Residential Internet Access Service, Broadband Network Operators should select, implement and locate equipment within the operator's architecture to provide residential internet access to the most users where economically and technically feasible.
- 7-7-0818 For the deployment of Residential Internet Access Service, Broadband Network Operators should deploy equipment that can report alarms.
- 7-7-0821 For the deployment of Residential Internet Access Service, a Broadband Network Operator should ensure that network deployment and equipment installation does not physically impair the operation of other collocated communications networks/equipment in the connection network (e.g., shared space in the outside plant).
- 7-7-0822 For the deployment of Residential Internet Access Service, a Broadband Network Operator should incorporate multilevel security schemes for network data integrity, as applicable, in the network design to prevent user traffic from interfering with network operations, administration, and management use.
- 7-7-0823 For the deployment of Residential Internet Access Service, Network Operators, Service Providers and Equipment Suppliers should design, build, and operate broadband networks considering performance aspects of the data facilities employed, such as: packet loss ratio, Bit Error Ratio, latency, and compression, where feasible.

F. Silent Failures

Another issue on which the Commission seeks comment pertains to silent failures, which are failures that happen when a malfunction makes detection difficult.[33] ATIS does not believe that these types of failures present a significant risk to network resiliency. The industry has existing practices in place to prevent and respond to such failures and providers closely monitor their networks in real time for such failures. Moreover, production links and chassis components are alarmed, comprehensive forwarding plane network monitoring is conducted, and the results of this monitoring are analyzed. As a result, the potential for "silent failures" has been minimized.

VI. THE NEED FOR COMMISSION ACTION

Finally, the Commission asks for input regarding potential barriers to implementation and ways to promote reliability and resiliency.[34] ATIS suggests that the Commission: (1) complete its work to redesign the Universal Service Fund so that funds can be made available for the building of robust broadband networks by providers whose coverage areas are in need of deployment, or upgrade, of broadband infrastructure;[35] and (2) continue its collaboration with the industry within ATIS NRSC and elsewhere to promote the development and use of voluntary Best Practices relating to reliability and resiliency.

[33] *NOI* at ¶41.

[34] *NOI* at ¶43.

[35] *Connect America Fund*, WC Docket No. 10-90; *A National Broadband Plan for Our Future*, GN Docket No. 09-51; *Establishing Just and Reasonable Rates for Local Exchange Carriers*, WC Docket No. 07-135; *High-Cost Universal Service Support*, WC Docket No. 05-337; *Developing an Unified Intercarrier Compensation Regime*, CC Docket No. 01-92; *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45; *Lifeline and Link-Up*, WC Docket No. 03-109, Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking (rel. February 9, 2011).

VII. CONCLUSION

ATIS continues to support the Commission's efforts to gain a better understanding of the operation of communications networks and to promote resilience and reliability. ATIS notes that the reliable provision of services to customers is a primary concern for service providers. Given the strong incentives that providers already have to provide reliable service, ATIS believes that further regulatory mandates in this area are not necessary or desirable. Instead, ATIS urges the Commission to provide the communications industry with the flexibility to meet evolving needs, new technologies and the broad spectrum of challenges that arise from a variety of man-made and natural disasters.

Respectfully submitted,

Alliance for Telecommunications Industry Solutions
By:

Thomas Goode
General Counsel

Dated: July 7, 2011