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

In the Matter of   )
)
The Proposed Extension of Part 4 of the   )   PS Docket No. 11-82
Commission's Rules Regarding Outage Reporting   )
to Interconnected Voice Over Internet Protocol   )
Service Providers and Broadband Internet Service   )
Providers   )

REPLY COMMENTS
OF THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

Thomas Goode
General Counsel
ATIS
1200 G Street, N.W.
Suite 500
Washington, D.C. 20005
(202) 434-8830

September 4, 2012

Table of Contents

In the Matter of	)
	)
The Proposed Extension of Part 4 of the	) PS Docket No. 11-82
Commission's Rules Regarding Outage Reporting	)
to Interconnected Voice Over Internet Protocol	)
Service Providers and Broadband Internet Service	)
Providers	)

**REPLY COMMENTS
OF THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS**

I.   Introduction and Summary

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' *Public Notice*, released July 18, 2012, in the above-referenced docket. ATIS

supports the Commission's efforts to develop a record of the facts surrounding the June 29,

2012, derecho storm that affected the Midwest, mid-Atlantic and Northeast regions of the

country. ATIS believes that this effort will facilitate a valuable dialogue among interested

stakeholders. As explained below, ATIS: (1) notes that the industry's existing collaborative

voluntary and consensus-based efforts to promote network reliability and resiliency have been

effective; (2) recommends that the suggestions that have been made for new industry practices be

reviewed by industry subject matter experts to ensure they are broadly implementable,

technically feasible and practical; and (3) urges the Commission not to allow direct access by

states to outage data collected by the Commission unless strong safeguards are in place to protect

this data.

II.   Background

ATIS is a global standards development and technical planning organization that develops 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, competitive local exchange carriers, providers of commercial mobile radio services, 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, which develop standards, specifications, best practices, guidelines, and other approaches as deemed essential to the operation and continued evolution of communications networks.

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, 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. These subject matter experts are the experts on communications reliability and outage reporting.

III.   **Voluntary Industry Efforts to Ensure Network Reliability and Resiliency Are Effective**

In the *Public Notice*, the Commission seeks comment on a number of issues related to the June 29, 2012, derecho storm that affected the Midwest, mid-Atlantic and Northeast regions of the country. Many of the questions asked by the Commission are appropriately directed at what additional steps can be taken to improve network reliability and robustness.[1] As explained below, ATIS believes that the industry's existing efforts to promote network reliability and resiliency, which focus on the development of voluntary, consensus-based standards, best practices, and public-private collaborative efforts, are effective.

As virtually all commenters have noted, the derecho storm was an extraordinary event. The storm was "extremely rare,"[2] "ferocious,"[3] and exacerbated by "a lack of advance warning and the region's unfamiliarity with derechos"[4] resulting in "unprecedented power outages and damage"[5] significantly greater than Hurricane Irene last year.[6] The extraordinary nature of the event stems not just from the type and path of the storm, but from its magnitude. T-Mobile USA, Inc. (T-Mobile) explained in its comments that the Connective Available Potential Energy (CAPE) levels associated with the June derecho storm – over 5,000 – were "astronomical" and well above the level associated with an extreme derecho storm.[7] The storm also produced the all-time highest recorded June or July wind gusts at several official observing sites along its

---

[1] See *Public Notice* at pp. 3-6.
[2] Comments of T-Mobile USA, Inc. at p. 2.
[3] Comments of Fairfax County, Virginia, at p. 18.
[4] Comments of AT&T at p. 4.
[5] Comments of Frontier Communications Corporation at p. 2 (quoting West Virginia Governor Earl Ray Tomblin).
[6] Comments of CTIA – The Wireless Association® at p. 6.
[7] Comments of T-Mobile at p. 2 (citation omitted).

path.[8] ATIS urges caution in drawing conclusions about network reliability and resiliency based on the unique circumstances of this event.

The comments clearly demonstrate that service providers take their responsibility to provide reliable services to consumers seriously and undertake significant efforts to prevent outages and restore service quickly. Service providers have emergency management and service restoration plans in place and these plans were effective even in the face of this extraordinary event.[9] AT&T Services, Inc. (AT&T) notes that "[d]espite the lack of advance warning, AT&T's wireless network performed well during and after the derecho."[10] T-Mobile similarly reports that, despite the hurricane strength winds, "the vast majority of T-Mobile's cell sites were operational the following day in the markets impacted by the storm. Network restoration occurred quickly because of the effective implementation of T-Mobile's disaster recovery policy and procedures."[11] Frontier Communications Corporation (Frontier) notes that, even though it did experience customer outages and impacts, "its West Virginia network performed with a high level of reliability and resiliency given the nature of the destruction."[12] Verizon and Verizon Wireless (Verizon) also report that their "rigorous network resiliency and service restoration practices largely worked as designed throughout most of the area affected by the Derecho."[13] The practices allowed Verizon to prevent "an overwhelming number of customers from losing

---

[8] *Id.*

[9] *See, e.g.* Comments of Frontier at p. 3, Comments of AT&T at p. 6, Comments of T-Mobile at p. 4, Comments of CTIA – The Wireless Association® at pp. 7-8.

[10] Comments of AT&T at p. 5.

[11] Comments of T-Mobile at p. 3.

[12] Comments of Frontier at p. 3.

[13] Comments of Verizon at p. 2.

service in the first instance, or… to trouble-shoot and remedy the causes of outages and restore service."[14]

While the significant efforts of service providers to maintain reliability and restore service cannot be disputed, neither can the fact that, despite these efforts, the derecho storm did impact communications networks and in some cases did result in outages. While providers engineer their networks to be extremely reliable, the fact is that no network can be designed or implemented to withstand every possible source of failure. This truism, however, does not mean that service providers are not looking for ways to improve reliability by examining existing practices in light of lessons learned from the derecho events. In fact, the opposite is true. The record in this proceeding shows that the service providers are actively engaged in significant efforts to review and, as appropriate, revise their existing practices to bolster reliability.[15]

Commenters also note that there are significant ongoing industry efforts to foster network reliability and resiliency and to mitigate the effects of natural disasters. CTIA – The Wireless Association® (CTIA) notes that its Business Continuity/Disaster Recovery Program provides an annual certification program for wireless carriers that have met planning standards and objectives necessary to ensure that they have prioritized service continuity and disaster recovery.[16] CTIA further acknowledges other industry efforts to foster network reliability including "the National Infrastructure Protection Plan, … the Communications Sector Coordinating Council, …the Alliance for Telecommunications Industry Solutions ('ATIS') Network Reliability Steering Committee ('NRSC') and the Commission's Communications Security, Reliability and

---

[14] *Id*. at pp. 1-2.
[15] *See* Comments of Frontier at p. 6, Comments of AT&T at p. 2, Comments of Verizon at p. 5.
[16] Comments of CTIA – The Wireless Association® at p. 7.

Interoperability Council."[17] The Telecommunications Industry Association (TIA) notes that "numerous voluntary intra- and inter-industry efforts, and public-private partnerships, undertake the task of network reliability continuously, producing standards and best practices that are heavily relied upon."[18] ATIS agrees with commenters that note that the existing voluntary and consensus-based standards, best practices, self-evaluation efforts, and public-private partnership efforts are the most effective way to promote network reliability and resiliency.[19]

These actions are not being taken because of regulatory mandates, but because the marketplace demands that service providers continuously maintain and enhance network reliability. ATIS agrees with TIA that the Commission should acknowledge that service providers have been dynamically improving reliability and resiliency and, as noted by the National Security Telecommunications Advisory Committee, "market incentives will remain the fundamental driver of industry practices and standards."[20] As T-Mobile notes, "[c]ompetitive market forces and strong dedication to servicing customers" ensure that carriers deploy and maintain reliable, resilient networks."[21]

The effectiveness of existing industry efforts are diminished by unnecessary regulatory mandates. By creating one size fits all solutions, regulatory mandates stifle the ability of carriers to modify practices to reflect lessons learned from events such as the derecho event, and to address the continued evolution of the network and the evolving needs of customers. As Verizon correctly notes, "the Commission has acknowledged [that]… network reliability best practices have evolved in a manner that accommodates flexibility in implementation while promoting

---

[17] *Id*. at pp. 8-9.
[18] Comments of TIA at p. 3.
[19] *See e.g.,* Comments of T-Mobile at p. 8, Comments of TIA at p. 3, Comments of Verizon at p. 14.
[20] Comments of TIA at p. 5 (quoting *National Security Telecommunications Advisory Committee Report to the President on Communications Resiliency* (rel. Apr. 19, 2011) at p. 4.)
[21] Comments of T-Mobile at p. 8.

meaningful improvements over time. Because of the necessarily iterative nature of this process, best practices, by design, cannot be readily translated into prescriptive rules."[22]

ATIS therefore agrees with T-Mobile's assessment that "[t]he experience gathered from the storm demonstrates that additional regulations are not necessary and that the voluntary industry efforts to ensure network reliability and resiliency are working effectively."[23]

IV.   **Back-Up Power Issues Should Be Addressed Through Existing, Voluntary Consensus-Based Efforts**

In the *Public Notice*, the Commission seeks input on what action it should take to address back-up power issues.[24] ATIS believes that the most effective way to address back-up power issues is through existing voluntary, consensus-based collaborative efforts.

Many commenters report that the implementation of back-up power mandates would face practical and legal hurdles. CTIA explains that, "[w]hile wireless carriers have made substantial investments in back-up power solutions, they have in many cases encountered significant obstacles in installing back-up power equipment at particular sites."[25] T-Mobile notes that the record in this proceeding demonstrates that "permanent backup power may not be possible at many sites due to factors beyond the control of carriers, such as space constraints, local zoning regulations, health and safety regulations, lease restrictions, *etc*."[26] Verizon similarly notes that back-up power is impacted by engineering design considerations, such as "how critical the site is for network coverage purposes, what equipment is installed at the site, neighboring site capacity and coverage overlap, availability of generator or other backup commercial power, and

---

[22] Comments of Verizon at pp. 14-15.
[23] Comments of T-Mobile at p. 8.
[24] *Public Notice* at p. 4.
[25] Comments of CTIA – The Wireless Association at p. 12.
[26] Comments of T-Mobile at p. 13.

environmental (e.g., space, weight, ventilation, landlord) concerns."[27] AT&T agrees and

explains that "[i]n addition to being inefficient, an on-site back-up power mandate could conflict

with other Federal, State, and local regulations ... [and] could be unsafe or impractical for many

facilities."[28]

Even if back-up power mandates could be implemented, these new mandates could have

a negative, rather than positive, impact on network resilience. In its comments, TIA correctly

notes that "the forced commitment of capital towards meeting reliability mandates, even in

instances where it is not appropriate for a facility, could better/otherwise be dedicated to best

addressing resiliency challenges as deemed appropriate by those with the best knowledge of

what a particular network needs to increase resiliency: the operator of that network."[29] AT&T

adds that new regulatory mandates, such as on-site back-up power requirements, "would divert

and dilute carrier resources that could otherwise be used more effectively in a disaster."[30] For

instance, T-Mobile explains that "[a] carrier that planned on investing in new cell sites to expand

coverage or improve capacity may be forced to forgo such deployment in order to satisfy

regulatory mandates regarding backup power."[31]

ATIS believes that service providers must retain the flexibility to determine how best to

maintain and restore power, and this includes determining how best to deploy back-up power. It

is this flexibility that is the key to ensuring that maintenance and restoration practices are tailored

to the unique needs of each service provider, each geographic area and each type of network-

impacting event. AT&T notes that its back-up power strategy "is based upon an assessment of

---

[27] Comments of Verizon at p. 16.
[28] Comments of AT&T at p. 9.
[29] Comments of TIA at p. 6.
[30] Comments of AT&T at p. 9.
[31] Comments of T-Mobile at p. 10.

local needs and characteristics, as well as an evaluation of what would be most efficient and effective for a given site. A regulatory mandate for on-site back-up facilities would eliminate a carrier's ability to conduct such an assessment and to determine, based upon actual results, the most effective way to restore all sites."[32] CTIA agrees that service providers should have the flexibility to make judgments regarding restoration/maintenance issues, including whether the deployment of cell base stations on wheels or cell base stations on light trucks are a better solution than a back-up power source in a particular case.[33] T-Mobile explains the need for carriers to have the flexibility to best determine how to restore and maintain communications. "If backup power is mandated, a wireless carrier may be forced to dedicate a specified amount of backup power at a site that may be unaffected by a natural disaster – as opposed to efficiently utilizing limited resources to purchase portable generators that can be quickly deployed to restore power to specific sites actually requiring alternative power."[34]

ATIS also notes that, even if back-up power regulations had been in place, it is not clear how effective they would have been in preventing communications outages. From the comments, it is clear that the derecho event did not just affect power – it damaged and destroyed communications lines, telephone poles and other infrastructure. Other network-impacting events came after the storm and were unrelated to the damage inflicted to communications networks by the derecho event. Frontier, in its comments, reports that "statewide power outages also cut off the supply of gasoline at many gas stations, making it difficult to find an adequate supply of gas to power all of the back-up generators."[35] ATIS therefore agrees with Frontier's conclusion regarding this matter – the use of back-up power sources like generators is "not a foolproof

---

[32] Comment of AT&T at p. 10.
[33] Comment of CTIA – The Wireless Association at p. 12.
[34] Comments of T-Mobile at p. 11.
[35] Comments of Frontier at p. 4.

solution."[36]

<h2>V.   ATIS Supports the Evaluation of Recommended Practices to Improve Reliability and Resiliency by the Industry</h2>

As noted above, ATIS strongly believes that voluntary industry-led efforts are the most effective way to promote network reliability and these efforts have proven their value time and time again, but particularly in light of the derecho event. A key element of these efforts is the development of industry best practices, which are voluntary industry practices that are developed through rigorous deliberation and expert consensus and proven through actual implementation.

Best practices are not "just good ideas" – they are industry practices that have been implemented by one or more industry participants and that have been confirmed by a broad set of stakeholders. It is also important to note that best practices are not applicable to all circumstances and therefore cannot be mandated. The Commission's Communications Security, Reliability and Interoperability Council (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.[37] 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.

---

[36] *Id*. at p. 4.

[37] 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).

ATIS notes that many of the service providers and other stakeholders have suggested practices that could be implemented to improve network reliability and service restoration.[38] ATIS supports the recommendation that the Commission should ask the existing CSRIC Working Group 8 to evaluate the practices proposed by various stakeholders and determine whether these practices warrant consideration by the industry as recommended best practices.[39] ATIS NRSC would also welcome the opportunity to evaluate these practices and provide its input to the CSRIC as appropriate.

Such review by industry subject matter experts would ensure that these practices are broadly implementable, technically feasible and practical. The review will also help to ensure that the practices are developed appropriately in accordance with the guidance provided by the Best Practices Tutorial, which has been created by the ATIS NRSC to promote the development of consistent and effective CSRIC best practices.[40] Finally, this industry review would help to ensure that any new practices are aligned with, and not duplicative to, existing industry practices. ATIS notes that its initial review of the practices recommended by stakeholders identified some potential overlap between the recommended practices and existing best practices. ATIS NRSC would be willing to undertake a more thorough examination of these recommended practices and their relationship to existing industry best practices.

VI.   **ATIS Urges the Commission Not to Allow Direct Access to NORS Data by States Unless Strong Safeguards Are in Place to Protect this Data**

Finally, ATIS notes that the California Public Utilities Commission (CA PUC), in its comments, urges the Commission to grant direct access to the data collected by the Commission

---

[38] *See, e.g.,* Comments of Fairfax County, Virginia at p. 23, Comments of Frontier at p. 6, Comments of the Association of Public-Safety Communications Officials-International, Inc. at p. 5, Comments of Verizon at p. 5.
[39] Comments of Verizon at pp. 7-8.
[40] The Best Practices Tutorial is publically available online at: http://www.atis.org/bestpractices/Tutorial.aspx.

through its Network Outage Reporting System (NORS).[41] With regard to state access to NORS

data, ATIS reiterates what it has said before – that strong safeguards must be in place before

direct access to NORS data could be granted.

As the Commission itself has noted "[t]he disclosure of outage reporting information to

the public could present an unacceptable risk of more effective terrorist activity because such

data could be used by hostile parties to attack communications networks."[42] In its petition for

state access to NORS data, the CA PUC agrees that outage data is sensitive and should be

protected.[43] Therefore, to protect this data, ATIS recommends that the following safeguards

should be in place before any state access could be considered:[44]

- States should not be permitted to share NORS data with: any governmental body that has
  not certified that it can protect such data; and any private entity, including private
  contractors that may be working on behalf of state agencies. Moreover, access to NORS
  data should be limited to state personnel with a need to know such information, and the
  copying or distribution of this data to others should be prohibited.

- Access to NORS data should only be permitted by states with laws in effect that would
  apply criminal penalties for misuse of NORS data.

- States should be required to have in place adequate policies and computer protections to
  ensure that outside parties are unable to procure access to such information from their
  servers or computers.

- There should be a limit to the number of personnel that may access the data and that the
  identities of those with such access should be kept on file with the Commission.

- The Commission should: (1) create and maintain an audit log for NORS to record what
  data was accessed, when and by whom; and (2) audit all NORS accounts granted to State
  Commissions and shut down those that have not been used for six months. Service

---

[41] Comments of the California Public Utilities Commission and the People of the State of California at p. 16.

[42] *Report and Order and Further Notice of Proposed Rulemaking*, ET Docket No. 04-35 (rel. August 4, 2004) at ¶3.

[43] See *Petition for Rulemaking*, filed November 12, 2009, by the California Public Utilities Commission and the People of the State of California (*CA PUC Petition*) (ET Docket 04-35, RM-11588) at p. 18.

[44] *See* ATIS Comments in response to the CA PUC Petition at pp. 5-6; see also ATIS Reply Comments in response to *CA PUC Petition* at pp. 4-6.

providers and other NORS filers should be provided with periodic reports on state access, including the number of active accounts and the number of reports accessed by each.

- To reduce the burden on service providers and eliminate the filing of duplicative information, direct state access to NORS data should not be afforded to states that have adopted reporting requirements that differ from those that have been adopted by the FCC.

- The use of NORS data by states should be limited to the purposes listed in the CA PUC petition, namely to allow the state "to perform its traditional role of protecting public health and safety through monitoring of communications network functionality."

- States should be required to provide employees with appropriate training regarding access to and use of NORS data.

- State Commissions should be required to inform the Commission and all affected NORS filers of any breach or suspected breach of data.

As previously recommended, ATIS believes that modifications to NORS would be required before direct state access to NORS could be provided. Because ATIS believes that individual states should only have access to data for providers and services that serve customers in the state and only for outages occurring in that state, regardless of the reporting party, NORS would have to be modified to allow a state to access only outage data affecting customers within that particular state. Similarly, modifications would be necessary to limit access only to outages affecting those services/providers regulated by the state.[45]

---

[45] *See* ATIS Comments in response to the CA PUC Petition at p. 7.

VII.   Conclusion

ATIS appreciates the opportunity to provide its input regarding this matter. As explained

above, based on the comments filed in this proceeding, ATIS does not believe that there is a need

for new Commission mandates related to network resiliency, reliability or back-up power. ATIS

believes that the existing voluntary industry efforts to ensure network reliability and resiliency

are working effectively. ATIS recommends that the suggestions that have been made for new

industry practices be reviewed by industry subject matter experts to ensure they are broadly

implementable, technically feasible and practical. Finally, ATIS urges the Commission not to

allow direct access by states to outage data collected by the Commission unless strong

safeguards are in place to this data.

Respectfully submitted,

ATIS

By: _____

Thomas Goode,
General Counsel
Alliance for Telecommunications Industry
Solutions
1200 G Street, N.W., Suite 500
Washington, D.C. 20005

Dated: September 4, 2012