

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matters of)	
)	
New Part 4 of the Commission’s Rules Concerning Disruptions to Communications)	ET Docket No. 04-35
)	
)	
Petition of California Public Utilities Commission and the People of the State of California for Rulemaking on States’ Access to the Network Outage Reporting System (NORS) and a Ruling Granting California Access to NORS)	RM-11588
)	
)	

COMMENTS

The Alliance for Telecommunications Industry Solutions (ATIS) hereby submits these comments on behalf of its Network Reliability Steering Committee (NRSC) in response to the *Petition for Rulemaking*, filed November 12, 2009, by the California Public Utilities Commission and the People of the State of California (*CA PUC Petition*). ATIS recognizes the legitimate needs of states to have access to outage reporting data, but believes that key issues must be addressed before direct state access to the Federal Communications Commission’s (FCC) Network Outage Reporting System (NORS) could be provided, including the need to ensure that NORS data remains confidential.

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. 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.

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.

II. If the FCC Establishes a Rulemaking to Examine State Access to NORs, Key Issues Must be Addressed

The ATIS NRSC and its members recognize that state regulatory agencies have legitimate needs to access outage reporting data. NRSC members operate in all fifty states,

the District of Columbia and in U.S. territories¹ and the members collaborate closely with state regulatory agencies to ensure that the nation's public networks maintain their vitality. When outages do occur, the members work to identify and, more importantly, to resolve the issue and to provide associated information regarding these efforts with the applicable state agencies. Nonetheless, given the sensitive nature of NORS data, ATIS believes that the FCC must carefully examine certain fundamental issues before it could consider providing states with direct access to NORS.

A. The Protection of NORS Data Must Be Assured

ATIS believes that any state access to NORS data must be contingent on certification by the state that it can adequately protect such critical data. ATIS notes that California in its petition does not disagree that outage data is sensitive or that it should be protected. However, ATIS does not believe that the *CA PUC Petition* sufficiently addresses potential concerns regarding confidentiality of this data and urges the FCC to address these concerns before granting any state direct access to NORS data.

In support of its petition, California notes that the FCC has previously granted states direct access to other "sensitive" data. It notes that the FCC has provided states with direct, passcode-protected access to numbering data in the North American Numbering Plan Administrator (NANPA) numbering utilization database.² While ATIS acknowledges that such access has been provided in other circumstances and for other data, ATIS does not believe that such access should necessarily be granted to all states for outage data. Outage reporting data is fundamentally different than numbering data in that its potential

¹ For the sake of simplicity, the term "state" is used in these comments to indicate U.S. states as well as the District of Columbia and U.S. territories.

² *CA PUC Petition* at p. 15.

public disclosure or misuse could pose significant risks to public safety and homeland security.

As the FCC noted in its August 2004 *Report and Order* adopting the new outage reporting rules, “[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.³ In deciding to keep outage reporting data confidential, the FCC also noted that “[t]he overwhelming majority of the commenting parties, including the Department of Homeland Security (‘DHS’), have demonstrated that the outage reports will contain sensitive data, which requires confidential treatment under the Freedom of Information Act (‘FOIA’).”⁴

The outage example provided in the *CA PUC Petition* demonstrates the potential risk posed if public disclosure of outage information were to occur. In that example, two cables were cut by vandals in the San Francisco Bay Area, resulting in an outage affecting wireline and wireless civilian, government, military and public services.⁵ If specific information regarding the outage was made publicly available, it could ultimately result in information (particularly the location and cause of the outage) that those looking to cause harm to a network may find valuable. Further, since once this information is disclosed to California it may reside on its servers, hackers or terrorists may be able to gain access to this information. As the number of computers and persons who have access to this information increases, so does the possibility that such information may be disclosed, even if inadvertently, to people with nefarious intentions.

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

⁴ *Id.*

⁵ *CA PUC Petition* at p. 14.

ATIS believes that the protections cited by California regarding Numbering Resources Utilization Forecast (NRUF) data are necessary but not sufficient to protect outage data. Therefore, in addition to requiring that the state have in place appropriate confidentiality protections and that any public disclosure or misuse be subject to the same or more stringent penalties that would apply to the misuse of numbering data, ATIS urges that additional safeguards be put in place. As an initial matter, access to NORS outage information should not compromise the FCC's protection of the information under FOIA. In addition, ATIS urges the FCC to ensure that the protection of data includes prohibitions against states' sharing of such 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. The FCC should also require that a state have laws in effect that would apply criminal penalties for misuse of NORS data. Further, 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. This would also require limiting access to such information to persons with a need to know such information, along with limitations on copying and distributing such information. Finally, if state-level direct access is granted, the FCC should establish a process by which service providers can seek redress from the FCC for any state misuse of outage reporting data.⁶

⁶ Such redress may include the termination of access to NORS by a state that misuses or fails to adequately protect NORS data.

B. Access to NORS Should Not Be Provided to States that have Outage Reporting Requirements that Differ from the FCC’s Requirements

In addition to restrictions pertaining to confidentiality, ATIS believes that the FCC should not grant direct state access to NORS data to states that have adopted reporting requirements that differ from those that have been adopted by the FCC.⁷ Further, states that are granted access to NORS should not require separate outage report filings or notifications that outage reports have been filed in NORS.

Limiting access, as stated above, would serve two important purposes. First, it will minimize confusion that occurs when separate reports that capture inconsistent outage reporting data are received (e.g., multiple outage impact counts, multiple reports for a single event, etc.). Second, it will minimize the burden on states and service providers, because they will not need to expend resources for separate data collection efforts or to differentiate between duplicative reports (i.e., one submitted to the FCC and another submitted to state).

C. Use of NORS Data Should be Limited to Protecting Health and Safety

Finally, ATIS believes that, should the FCC grant state-level direct access to NORS data, use of such outage reporting data 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.”⁸

⁷ 47 CFR §4.1 *et seq.*

⁸ *CA PUC Petition* at p.14.

III. Before Direct State Access to NORS Could Be Provided, the FCC Must Make Modifications to this System

In its petition, California notes that “[b]ased on discussions with FCC staff, it appears that providing the CPUC access to the NORS database would be relatively straightforward.”⁹ ATIS disagrees and notes that, if a decision were made to permit direct state access to NORS, significant changes to the system would be necessary.

For instance, 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. ATIS believes therefore that 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. ATIS also believes that additional NORS modifications may be necessary to permit states access only to data pertaining to outages that occur after the state has been granted access to NORS.

To avoid confusion and minimize the burden on states and service providers, ATIS recommends two additional modifications to NORS should direct state access be provided. First, the primary and secondary contact information listed in NORS should be redacted from state viewable events because this information identifies service provider personnel that may be responsible only for FCC outage reporting in NORS. Many service providers have different state specific personnel assigned to address and/or respond to state outage reporting issues. The failure to redact this primary and secondary contact information could cause confusion and potentially delay responses to the FCC and state inquiries.

⁹ *Id.* at p.13.

Second, NORS notifications that new or modified outage reports have been submitted by a service provider in a given state should be sent directly to any state that has been granted access.¹⁰ ATIS notes that such notifications will ensure that any state that has been granted access to NORS is automatically kept apprised of pertinent outage reports. This notification would also substantially reduce the burden on service providers to provide a separate state notification every time they submit a NORS report.

IV. Conclusion

ATIS urges the FCC not to grant direct state access to NORS without full consideration of the issues noted above. In particular, ATIS urges the FCC to ensure that any state access to NORS data is contingent on certification by the state that it can adequately protect such critical data. In addition, the FCC should not grant direct state access to NORS data to states that have adopted reporting requirements that differ from those that have been adopted by the FCC. Finally, ATIS notes that changes to NORS would be required before state access could be provided to appropriately limit the scope of access, to minimize the likelihood of confusion and to reduce the burden on both service providers and states.

¹⁰ State access should be limited to the four primary report statuses: notification, initial, final and withdrawal.

Respectfully submitted,

Alliance for Telecommunications Industry Solutions

By:



Deirdre Cheek
Attorney



Thomas Goode
General Counsel

Dated: March 4, 2010