

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 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

R. _____

**PETITION OF
THE CALIFORNIA PUBLIC UTILITIES COMMISSION
AND THE PEOPLE OF THE STATE OF CALIFORNIA
FOR RULEMAKING ON STATES' ACCESS TO THE NETWORK OUTAGE
REPORTING SYSTEM ("NORS") DATABASE AND
A RULING GRANTING CALIFORNIA ACCESS TO NORS**

FRANK R. LINDH
HELEN M. MICKIEWICZ
HIEN C. VO
505 Van Ness Avenue
San Francisco, CA 94102
Phone: (415) 703-1319
Fax: (415) 703-4432
Email: hcv@cpuc.ca.gov
Attorney for the California
Public Utilities Commission And The
People of the State of California

November 12, 2009

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. BACKGROUND	3
A. FCC Outage Reporting Requirements Under New Part 4 Rules	3
B. California Streamlines Outage Reporting Requirements to Conform to FCC NORS Reports	5
III. DISCUSSION	7
A. The FCC Has Not Precluded States From Directly Receiving NORS Reports.....	9
1. The Commission Contemplated Intergovernmental Sharing of NORS Disruption and Outage Reports.....	9
2. Obtaining NORS Reports From DHS Is Neither A Practical Nor Efficient Alternative to Direct Access to the NORS Database.....	12
B. Direct Access to FCC NORS Reports is Critical to California.	13
C. California’s Request is Reasonable Considering the FCC Granted It Similar Access to the Confidential NANPA Database.	15
D. California Can Adequately Safeguard NORS Reports From Public Disclosure.	18
IV. CONCLUSION.....	20

The California Public Utilities Commission (“CPUC” or “California”) submits this Petition for Rulemaking to the Federal Communications Commission (“FCC” or “Commission”) pursuant to 47 C.F.R. § 1.401. In this petition, the CPUC requests that the FCC grant state public utilities commissions direct access to the FCC’s Network-Outage Reporting System (“NORS”) database under the Commission’s rules in *New Part 4 of the Commission’s Rules Concerning Disruptions to Communications; ET Docket No. 04-35, Report and Order*¹ (“New Part 4 Rules”). Additionally, pursuant to 47 C.F.R. § 1.41, the CPUC requests password-protected access to the NORS database; such access would be expressly limited to California-specific disruption and outage data.

I. INTRODUCTION

NORS is the Internet-based filing system through which communications service providers covered by the *New Part 4 Rules* electronically report information about significant disruptions or outages to their communications systems when specified thresholds are met. The Commission implemented NORS after the September 11, 2001 terrorist attacks to help ensure stable, reliable communications in crisis situations.² In the *New Part 4 Rules*, the FCC granted the Department of Homeland Security (“DHS”) direct access to NORS information and acknowledged that release of the NORS reports by DHS

¹ *In the Matter of New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, Report and Order and Further Notice of Proposed Rulemaking*, 19 FCC Rcd. 16830 (2004) (“New Part 4 Rules Report and Order”).

² *Id.*

to other governmental agencies may be appropriate.³ However, the Commission was silent as to whether it would grant other governmental agencies the same access to NORS information.

Access to the NORS database is critical to California, which recently streamlined its reporting scheme for communications disruptions and outages by conforming them to the FCC's NORS reports. Allowing California direct access to the NORS database would eliminate redundant reporting schemes across different levels of government and among multiple states.⁴ Further, access to NORS would enable California to rapidly obtain complete and accurate information on service disruptions. This is vital to support California's homeland security and emergency response functions.

Moreover, the Commission need not be concerned with public disclosure of NORS data should it grant the CPUC's request. California has adequate laws and rules in place to safeguard confidential information, as exemplified by its protection of confidential numbering data obtained from the FCC. Indeed, the FCC already has allowed California (and other states) routine password-protected access to data collected in Numbering Resources Utilization Forecast ("NRUF") reports, which are maintained by the North American Numbering Plan Administrator ("NANPA") in a confidential database. In this petition, the CPUC proposes a similar arrangement for its access to NORS.

³ *Id.* ¶ 47, at 16856.

⁴ California recognizes that other states may have similar needs and/ or interests regarding access to the NORS database. Nonetheless, California does not purport to speak here for other states, and is filing this request on its own behalf.

II. BACKGROUND

A. FCC Outage Reporting Requirements Under New Part 4 Rules

The Communications Act charges the FCC with overseeing the reliability and security of the Nation’s telecommunications network.⁵ In 1992, the FCC first adopted voluntary outage reporting rules for the wireline telecommunications industry to enable the Network Reliability Council, other carriers, and manufacturers to be able to understand the causes of outages and to adequately address them to avert future outages with similar causes.⁶ The outage reports voluntarily filed under these original rules were generally available to the public.⁷

In 2004, following the terrorist attacks of September 11, 2001, the FCC adopted mandatory outage reporting requirements known as the *New Part 4 Rules*. In the underlying proceeding, the Commission recognized the critical need for “rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of the Nation’s communications networks and critical infrastructure.”⁸ Finding that mandatory reporting of network outages was “the only reliable way to collect this important information *for use by this*

⁵ *Id.* ¶ 12, 32, at 16837.

⁶ *Memorandum Opinion and Order, In re MSNBC Interactive News, LLC*, 23 FCC Rcd. 14518, ¶ 2 (2008) (“MSNBC Order”), *citing* Notification by Common Carriers of Service Disruptions, 7 FCC Rcd. 2010 (1992); 8 FCC Rcd. 8517 (1993); 9 FCC Rcd. 3911 (1994); and 10 FCC Rcd. 11764 (1995) adopting former 47 C.F.R. Part 63.

⁷ *Id.* at 14519.

⁸ *New Part 4 Rules Report and Order*, 19 FCC Rcd. 16830, ¶ 1 (2004).

*Commission and, where appropriate, for other government entities,”*⁹ the Commission extended reporting to all communications providers that provide voice and/or paging communications.¹⁰

Under the *New Part 4 Rules*, the FCC mandated carriers to submit outage reports electronically via NORS.¹¹ NORS utilizes a "fill in the blank" template that allows carriers to electronically submit their service outage reports to the FCC. In addition, the FCC uses a common metric to establish a general outage-reporting threshold for all covered communications providers.¹²

In contrast to its earlier policy of public disclosure, the FCC determined in the *New Part 4 Rules* that outage reports containing sensitive data would require confidential treatment under the Freedom of Information Act (“FOIA”).¹³ To support its change in policy, the FCC found that the national defense and public safety goals that it sought to achieve by requiring these outage reports would be seriously undermined if it were to permit these reports to fall into the hands of terrorists who seek to cripple the nation’s communications infrastructure.¹⁴ In addition, the FCC articulated the following reasoning:

⁹ *Id.* ¶ 32 , at 16848. (emphasis added).

¹⁰ *Id.* ¶ 2, at 16834.

¹¹ *Id.*; see also Network Outage Reporting System, <http://www.fcc.gov/pshs/outage/> (last visited Oct. 23, 2009).

¹² *New Part 4 Rules Report and Order*, 19 FCC Rcd. 16830 (2004).

¹³ *Id.* ¶ 3, at 16834.

¹⁴ *Id.* ¶ 45, at 16855.

[R]elease of this information could also make regulated entities less forthright in the information submitted to the Commission at a time when it is especially critical that we obtain full and accurate information in order to prevent harm to the communications infrastructure.¹⁵

While the FCC amended its rules to prevent disclosure of the confidential NORS reports to the public,¹⁶ at the same time, it granted DHS's request for direct access to these same reports. Reasoning that direct receipt of the outage information was necessary for DHS to fulfill its responsibilities under the Homeland Security Act, the FCC stated it would make available to DHS, in encrypted form and immediately upon receipt, all electronically submitted outage reports.¹⁷ However, no state public utility commission made a request for access to NORS during the *New Part 4* proceeding. As a consequence, the FCC was silent as to whether it should or would grant state public utilities commissions the same direct access to the NORS reports as it had given to DHS.¹⁸ Instead, the Commission concluded that DHS could share information from those reports with other government authorities that DHS deemed appropriate.¹⁹

B. California Streamlines Outage Reporting Requirements to Conform to FCC NORS Reports

California law requires every public utility to furnish and maintain adequate, efficient, just, and reasonable service, equipment, and facilities, necessary to promote the

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.* ¶ 47, at 16856.

¹⁸ *Id.* ¶ 25, at 16845, ¶ 47, at 16856. While the Commission articulates DHS's recommendation that state public utility commissions should receive the outage reports, the Commission does not directly respond to the recommendation.

¹⁹ *Id.* ¶ 47, at 16856. (footnote omitted).

safety, health, comfort, and convenience of the public.²⁰ Frequent or widespread service outages pose a potential significant threat to public safety,²¹ as well as tremendous inconvenience to all users of communications services. Tracking and reporting major service interruptions continues to be an important way for the CPUC to be apprised of service interruptions that may affect public safety, and to assess changes that may be necessary to ensure that the public receives adequate, efficient, just, and reasonable telephone service, including uninterrupted access to 911 emergency services.²²

Balancing California's need for robust service outage reporting and a policy favoring streamlined reporting requirements, the CPUC determined in Decision (D.) 09-07-019, issued July 16, 2009, that it could achieve both objectives by adopting the FCC's NORS reporting requirements.²³ Decision 09-07-019 eliminated California-specific guidelines for disruption and outage reports and replaced those guidelines with the FCC NORS guidelines. Three of the four largest Incumbent Local Exchange Carriers ("ILECs") in California, AT&T, Surewest, and Frontier, in comments filed with the CPUC, supported California's move towards reliance on the FCC's NORS reporting scheme.²⁴

²⁰ Cal. Pub. Util. Code § 451.

²¹ Order *Instituting Rulemaking on the Commission's Own Motion into the Service Quality Standards for All Telecommunications Carriers and Revisions to General Order 133-B*, R.02-12-004, 2002 Cal. PUC LEXIS 868 at 55.

²² *Id.* at 56.

²³ *Decision Adopting General Order 133-C and Addressing Other Telecommunications Service Quality Reporting Requirements*, D.09-07-019, 2009 Cal. PUC LEXIS 320.

²⁴ *Id.* at 61-2.

Because the CPUC does not currently have access to the NORS database, D.09-07-019 requires all facilities-based certificated and registered telecommunications providers to concurrently report to the CPUC all information electronically submitted to the FCC under NORS, when California service is affected.²⁵ The CPUC requirement is unnecessarily duplicative and inefficient. The CPUC's preferred method of obtaining access to California-only outage and disruption data through password-protected access to the FCC's NORS database, would be faster, more efficient, and would not require the carriers to submit the same material to two separate agencies.²⁶ Password-protected access to NORS would eliminate redundant reporting and ensure uniform and comprehensive reporting by service providers.

III. DISCUSSION

The receipt of information about communications disruptions is no less critical to state regulatory commissions than it is to the FCC. As discussed below, the FCC should allow California direct password-protected access to the NORS database.²⁷ This will ensure that the CPUC can rapidly and effectively coordinate its efforts to maintain or restore communications services at the local, state, and federal level.

In the FCC's *New Part 4 Rules Report and Order*, the FCC recognized the vital need for reliable communications during times of crises. To illustrate, the Commission

²⁵ *Id.* at 64.

²⁶ *Id.*

²⁷ Rather, the FCC simply did not address the question of state access to NORS.

discussed the types and levels of communications services used by emergency responders during and after the September 11, 2001 terrorist attacks.

First responders and medical personnel were notified by pagers, cellular telephones, wireline telephones, and the Internet of the tragic events that had occurred, and were occurring, and the immediate need for their services. When these services failed or were overwhelmed, first responders sometimes found themselves falling back on old fashioned ‘messenger’ tactics. Long distance communications, including satellite communications, were used to initiate the movement of equipment and personnel into the affected areas for restoration purposes and to coordinate their work. *All levels of government (municipal, county, state, and Federal) coordinated their restoration and Homeland Defense efforts through wireless and wireline phones, public data networks (including dial-up telephone, wireless, can cable modem access to the Internet), and pagers.* In this context, the need for immediate, secure, and reliable communications service is obvious.²⁸

The Commission also acknowledged the nation’s complete dependency on communications services essential to the operation of virtually all government, business, and critical infrastructures throughout the United States.²⁹

Consider, for example, our financial infrastructure which, in large measure, consists of computers, databases, and communications links. If the communications links were severed, or severely degraded, ATM machines would not be able to supply cash, credit card transactions would not ‘go through,’ banks would not be able to process financial transactions (including checks), and the financial markets would become dysfunctional. In a short time, economic activity would grind to a halt and consumers’ ability to purchase food, fuel or clothing would be severely limited if not destroyed. This single example leads, ineluctably, to the

²⁸ *New Part 4 Rules Report and Order*, 19 FCC Rcd. 16830, ¶ 10, at 16836 (2004) (footnotes omitted) (emphasis added).

²⁹ *Id.* ¶ 11, at 16836.

conclusion that the people of the United States must have secure communications that they can rely upon for their daily needs, as well as during terrorist attacks, fires, natural disasters (such as hurricanes, earthquakes, and tornadoes) and war.³⁰

For these reasons, the FCC found that it was required “to obtain information about communications disruptions and their causes to prevent future disruptions that could otherwise occur from similar causes, as well as to facilitate the use of alternative communications facilities while the disrupted facilities are being restored.”³¹ These reasons equally apply to California.

A. The FCC Has Not Precluded States From Directly Receiving NORS Reports.

1. The Commission Contemplated Intergovernmental Sharing of NORS Disruption and Outage Reports.

Intergovernmental sharing of information on communications outages and disruptions is necessary to both state and local governments. The Commission recognized this when it stated in the *New Part 4 Rules Report and Order* that upon receipt of the NORS reports, DHS could “undertake to provide information from those reports to such other governmental authorities as it may deem to be appropriate.”³² The FCC also stated that “the mandatory reporting of network outages is the only reliable way to collect this important information for use by this Commission, and where appropriate, for other government entities.”³³ The Commission’s decision to specifically grant DHS

³⁰ *Id.* ¶ 11, at 16836-7 (footnotes omitted).

³¹ *Id.* ¶ 11, at 16836.

³² *New Part 4 Rules Report and Order*, 19 FCC Rcd. 16830, ¶ 47, at 16856 (2004).

³³ *Id.* ¶ 32, at 16848.

access to NORS reports, however, should not be interpreted as a bar against direct access to those reports by other governmental agencies.

On the contrary, the record in the underlying proceeding, which included comments from DHS, demonstrates that that the FCC should make outage information available to governmental entities other than DHS. At the state level, DHS specifically recommended that the Commission should

explore methods to make outage information available to State public utility commissions, in order to assure that State authorities have the outage data they need to support their homeland security and emergency response functions, reduce the need for State regulators to collect intrastate outage data independently, and to reduce the reporting burden on communications providers.³⁴

DHS further argued that much of the reported data would likely constitute homeland security information under Federal law, stating that “sharing the information with State authorities through such channels would also facilitate more effective safeguarding of this sensitive information against disclosure to those who might desire to use it for hostile purposes.”³⁵ Significantly, none of the other commenting parties directly challenged any of DHS’s comments in the underlying proceeding.³⁶

At the local level, the FCC recognized that local governments may also have a need for outage information. The Commission cited to comments made by the City of New York, the National League of Cities, and the National Association of

³⁴ *Id.* ¶ 25, at 16845.

³⁵ *Id.* ¶ 47, at 16856 n.145.

³⁶ *Id.* ¶ 20, at 16842 n.44.

Telecommunications Officers and Advisors (“City of New York *et al.*”) as support, which specifically noted the importance of local governments being promptly informed of network outage information affecting their jurisdictions.³⁷

[G]iven local government’s limited regulatory authority over the industry, local government should not have to be put in the position of being primarily responsible for tracking down and assessing the validity of the many, and often conflicting, explanations by wireline and wireless carriers for such potentially devastating outages. Rather, mandatory and adequate service outage reporting requirements imposed and enforced by the FCC would help relieve local governments of this burden and ensure uniform and comprehensive reporting by *all* affected service providers.³⁸

In its comments, DHS agreed with the sentiment of comments from the City of New York *et al.*³⁹

Similar to the FCC, state commissions are also responsible for overseeing the reliability and security of their state’s respective communications infrastructures. In times of crisis or in emergency situations, local and state authorities are often the first responders. Therefore, the Commission could take a step towards ensuring that its efforts to maintain the Nation’s telecommunications infrastructure are consistent at the lower levels of government by allowing California to access the uniform outage reports contained in the NORS database.

³⁷ *Id.* ¶ 32, at 16848 n.104.

³⁸ *Id.*, *citing* to City of New York *et al.* Joint Comments at 7-8.

³⁹ *Id.* ¶ 32, at 16848 n.104.

2. Obtaining NORS Reports From DHS Is Neither A Practical Nor Efficient Alternative to Direct Access to the NORS Database.

It is neither practical nor efficient for the CPUC to obtain from DHS information in the NORS database. Indeed, expecting states to ask DHS for this information, or for DHS to provide it, is unreasonable. The FCC collects the information, maintains the database, and provides information to DHS at its request. Requiring states to seek the information from a third party (DHS) would add another unnecessary step to California's efforts to obtain and review the data in NORS. This, in turn, would both lengthen the time and complicate the process for states to obtain the information. It simply is not logical for the CPUC to obtain FCC NORS outage reports secondhand from DHS.

Currently, pursuant to CPUC order,⁴⁰ wireline carriers under the CPUC's jurisdiction provide NORS reports to the CPUC staff via e-mail. Since July 2009, when the CPUC required carriers to provide copies of NORS reports, staff has received approximately 115 reports per month. This process requires that staff open each email and input the data into a database before it can analyze the outage data. This is neither a practical nor efficient use of staff resources. In addition, it requires the carriers to provide information to the FCC and then separately to provide copies to the CPUC.⁴¹ Access to the FCC NORS database would allow the CPUC to download outage

⁴⁰ D.09-07-019, 2009 Cal. PUC LEXIS 320.

⁴¹ It is worth noting that, without access to NORS, the CPUC has no ability to determine if the information provided to the CPUC is identical to the information provided to the FCC, which is then input into NORS.

information in Excel format and then spend time and resources analyzing the data, as opposed to expending significant resources first having to input data.

Further, the FCC has regulatory authority over the entities providing the information to the Commission, while DHS has no such authority. Thus, in the event a dispute should arise over state access to NORS, or a state were to identify deficiencies in a particular carrier's data, or a carrier wished to object to a particular state's access to data, DHS would not be positioned either to resolve the issue(s) raised, or to compel production or refinement of data.

Based on CPUC staff discussions with FCC staff, it appears that providing the CPUC access to the NORS database would be relatively straight-forward. Once the CPUC gained access to NORS, FCC staff would not need to devote much, if any, ongoing effort beyond the work necessary to maintain the database. Additionally, CPUC access to NORS would reduce the burden on the carriers to send the NORS reports to the CPUC.

B. Direct Access to FCC NORS Reports is Critical to California.

The public health and safety, as well as California's economy, depend heavily on reliable and well functioning wireline and wireless voice and data communications networks. These networks are virtually ubiquitous, interconnected, and interdependent. It is critical that the CPUC have access to the level of service outage detail found in the NORS reporting in order to analyze effectively the data. Comprehensive analysis is key

to understanding the affect of outages on the multiple modes of communication and data services which comprise the state's communications network(s).

To illustrate the need for outage information, the FCC need only consider a major outage earlier this year in the San Francisco Bay Area. On April 9, 2009, six AT&T fiber optics cables were cut by vandals in two locations in the Bay Area, about 40 miles apart. These cables served wireline telephone service, wireless telephone service, computer networks, and Internet access services. These same facilities are also used for inter-and intra-communication company data and control systems. Civilian, government, military, and public safety services were affected, with service not fully restored in some areas for 24 hours. The perpetrators gained access to the fiber optic cables through manhole covers in public streets, where access apparently, was not sufficiently secure.

NORS outage data contains information that would help evaluate the cause of the outages such as the April 9, 2009 incident in California. The CPUC could analyze the NORS data to determine whether an incident of this type is a one-time occurrence, outside the control of the utility. Alternatively, the incident might indicate a broader organic and/or systemic problem with certain facilities that should be investigated on a carrier-specific, industry-segment, or industry-wide basis to determine what, if any, corrective measures need to be taken. California's goal here is simply to obtain the data necessary to perform its traditional role of protecting public health and safety through monitoring of communications network functionality.

C. California’s Request is Reasonable Considering the FCC Granted It Similar Access to the Confidential NANPA Database.

In the FCC’s *Numbering Resource Optimization* (“NRO”) proceeding, CC Docket No. 99-200, the FCC sought to slow the rate of number exhaust (assignment of area codes) in the U.S. and to prolong the life of the North American Numbering Plan (NANP).⁴² The North American Numbering Plan Administrator (“NANPA”) maintains a database of carrier number inventories which carriers report semi-annually in their Numbering Resources Utilization Forecast (“NRUF”) reports. The NANPA maintains the database, updating it after the semi-annual reports are submitted. The FCC and the states rely on this same data to monitor carrier use of telephone numbers, which the FCC has deemed a “public resource.”⁴³

Among the many issues the FCC considered in the *NRO* docket was whether state Commissions should have access to the NANPA database and, if so, what, if any, special provisions should be established to protect the confidentiality of data disclosed to the NANPA, the FCC, and state commissions. The FCC noted that under Exemption 4 of

⁴² For a complete summary of the history of the *NRO* proceeding, see *In the Matter of Numbering Resource Optimization*, Report and Order and Further Notice of Proposed Rulemaking, 15 FCC Rcd. 7574, 7577-82, ¶’s 1-9 (2000) (“NRO Report and Order”); see also *In the Matter of Numbering Resource Optimization; Petition for Declaratory Ruling and Request For Expedited Action on the July 15, 1997 Order of the Pennsylvania Public Utility Commission Regarding Area Codes 412, 610, 215, and 717*, Second Report and Order, Order on Reconsideration in CC Docket No. 96-98 and CC Docket No. 99-200, and Second Further Notice of Proposed Rulemaking in CC Docket No. 99-200, 16 FCC Rcd. 306, 310, ¶’s 4-17 (2000) (“NRO Second Report and Order”).

⁴³ *In the matter of High-Cost Universal Service Support*, Order on Remand and Report and Order and Further Notice of Proposed Rulemaking, 24 FCC Rcd. 6475, ¶ 111, at 6545 (2008) (“Telephone numbers are a finite, public resource.”)

FOIA, the FCC need not disclose commercial or financial information that is privileged or confidential.

The FCC found that states have legitimate reasons for obtaining disaggregated, carrier-specific data reported to NANPA.⁴⁴ The ability of the state commissions to perform duties pursuant to authority the FCC has delegated to the states⁴⁵ regarding area code relief would be hampered if states were not allowed access to carrier forecast and utilization information.⁴⁶ In so doing, the FCC recognized the significant role the states play in ensuring that area code relief planning is responsive to public need.⁴⁷

In the FCC's *Second Report and Order* in the *NRO* proceeding, the FCC clarified the scope of state access to carriers' NRUF data. Specifically, the FCC determined that "states shall have access to *all* such mandatorily reported data received by NANPA."⁴⁸

In the FCC's *Third report and Order*, the FCC held that "state commissions should have password-protected access to the NANPA database for data pertaining to NPA's

[numbering plan areas] located within their state. Each state commission...must maintain

⁴⁴ *In the Matter of Numbering Resource Optimization*, Report and Order and Further Notice of Proposed Rulemaking, 15 FCC Rcd. 7574, ¶ 75, at 7606 (2000) ("The states are responsible for NPA relief decisions and other delegated number issues. Such decisions must be based on specific utilization data. We are convinced that state commissions will be better able to meet their obligations with respect to area code relief with the information that we have determined is necessary.")

⁴⁵ *Id.* ¶ 81, at 7608.

⁴⁶ *Id.*

⁴⁷ See *supra* note 40.

⁴⁸ *In the Matter of Numbering Resource Optimization*, Third Report and Order and Second Order On Reconsideration, 17 FCC Rcd. 252, ¶ 133, at 309 (2001) (emphasis added) *citing In the Matter of Numbering Resource Optimization; Petition for Declaratory Ruling and Request For Expedited Action on the July 15, 1997 Order of the Pennsylvania Public Utility Commission Regarding Area Codes 412, 610, 215, and 717*, Second Report and Order, Order on Reconsideration in CC Docket No. 96-98 and CC Docket No. 99-200, and Second Further Notice of Proposed Rulemaking in CC Docket No. 99-200, 16 FCC Rcd. 306, ¶ 151, at 369 (2000).

the confidentiality of carrier-specific data as set forth in the *First Report and Order*.⁴⁹

In other words, “any state that cannot certify its ability to keep such data confidential shall not have access, password-protected or otherwise.”⁵⁰

The FCC’s reasons for allowing states direct access to NANPA also apply to the CPUC’s request to access the NORS database. The FCC’s *Third Report and Order* states in relevant part:

The advantages of providing states with password-protected access to forecast and utilization data include the ability to access data on a more timely basis, and access to the data in a format that allows manipulation of the data and the creation of customized reports. *We conclude that such access will only enhance the ability of states to determine when and what area code relief is necessary.* Further, we do not believe that allowing state commissions password-protected access to carrier-specific forecast and utilization data will pose any greater security risks than the current reporting system, in which NANPA distributes this data in semi annual reports. *Moreover, we find that the value to state commissions of timely access to forecast and utilization data outweighs the confidentiality concerns expressed by the carriers required to submit this data to the NANPA.*⁵¹

Moreover, should the FCC require, the CPUC could certify that it has appropriate protections in place, as discussed below, that would preclude disclosure of confidential NORS data to the public.

⁴⁹ *Id.* ¶ 133, at 309 (2001).

⁵⁰ *Id.* ¶ 136, at 310. California provided evidence of its statutory provisions protecting carrier confidentiality and was granted access to the NANPA database.

⁵¹ *Id.* ¶ 135, at 309-310 (emphasis added).

D. California Can Adequately Safeguard NORS Reports From Public Disclosure.

The CPUC recognizes that public disclosure of disruption and outage data contained in the NORS reports poses serious implications to the nation's critical information infrastructure. Therefore, consistent with the FCC's treatment of NORS data, the CPUC ordered in D.09-07-019 that it would treat such information as confidential pursuant to the CPUC's well-established protections under California Public Utilities ("P.U.") Code § 583 and CPUC General Order ("G.O.") 66-C.

P.U. Code § 583 makes it a criminal offense for any employee of the CPUC to release confidential information to the public. Under section 583,

no information furnished to the commission by a public utility, or any business which is a subsidiary or affiliate of a public utility, or a corporation which holds a controlling interest in a public utility, except those matters specifically required to be open to public inspection by this part, shall be open to public inspection or made public except on order of the commission, or by the commission or a commissioner in the course of a hearing or proceeding. Any present or former officer or employee of the commission who divulges any such information is guilty of a misdemeanor.⁵²

Because the CPUC afforded NORS information confidential treatment in D.09-07-019, the information would not be open to public inspection.

G.O. 66-C further protects from public inspection "records or information of a confidential nature furnished to, or obtained by the Commission."⁵³ Examples of "information of a confidential nature" and thus withheld from public disclosure, include

⁵² Cal. Pub. Util. Code § 583.

⁵³ CPUC General Order No. 66-C § 2 (June 5, 1974).

“[n]on-public communications with other public agencies or officers where the public interest in withholding such records ‘clearly outweighs the public interest in disclosure.’”⁵⁴ NORS data would clearly fall into this category. Therefore, G.O. 66-C would further protect NORS data from public disclosure.

Finally, in the FCC’s *NRO* proceeding, the FCC agreed with carriers that the NANPA data would contain “highly sensitive ‘commercial information’ and would in effect provide competitors access to their business plans and strategies, location of customers, expansion plans and market growth.”⁵⁵ Therefore, the FCC found that “disaggregated, carrier-specific forecast and utilization data should be treated as confidential and should be exempt from public disclosure under U.S.C. § 552(b)(4) [trade secrets].”⁵⁶ For that reason, the FCC granted all states access to the disaggregated data submitted to the NANPA, but required any state seeking access to NANPA to have in place appropriate confidentiality protections. The FCC declined to require a specific mechanism to ensure confidential treatment.⁵⁷ Similarly, other states seeking access to NORS reports under the proposed rule in this petition would be required to show sufficient protection for the confidential information.

Since the FCC granted California access to the NANPA database, the CPUC continues to utilize the information obtained from NANPA to oversee the utilization of

⁵⁴ *Id.* at § 2.4.

⁵⁵ *In the Matter of Numbering Resource Optimization*, Report and Order, 15 FCC Rcd. 7574, ¶ 78, at 7607 (2000).

⁵⁶ *Id.*

⁵⁷ *Id.*

area codes in California. Moreover, the CPUC has never released the confidential NANPA data to the public. Therefore, the FCC need not be concerned that California would treat any less seriously the importance of safeguarding confidential information contained in the NORS reports.

IV. CONCLUSION

In order to maintain the reliability and security of the Nation's telecommunications network, the FCC should permit direct-access by state public utilities commissions to the outage reports contained in the NORS database under the Commission's *New Part 4 Rules*. As articulated in this petition, the rapid receipt of comprehensive and uniform data concerning communications disruptions is no less critical to state regulatory commissions than it is to the FCC. Moreover, obtaining the NORS reports from DHS would not be a practical, nor efficient alternative to the CPUC's proposed rule. Finally, the Commission should grant the CPUC's request for password-protected access to California-only outage and disruption data in the NORS database. California has appropriate confidentiality protections in place to prevent the public disclosure of NORS data.

By: /s/ HIEN C. VO

Hien C. Vo

505 Van Ness Avenue
San Francisco, CA 94102
Phone: (415) 703-1319
Fax: (415) 703-4432
Email: hcv@cpuc.ca.gov

Attorney for the People
Of The State Of California And The
California Public Utilities Commission

November 12, 2009