Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
SPECIAL ACCESS FOR PRICE CAP LOCAL EXCHANGE CARRIERS	)	**WC Docket No. 05-25**
	)	
	)	

OPPOSITION OF THE INDEPENDENT TELEPHONE & TELECOMMUNICATIONS ALLIANCE

The Independent Telephone & Telecommunications Alliance ("ITTA") hereby submits its Opposition to the National Cable & Telecommunications Association's ("NCTA's") Application for Review[1] of the September 18, 2013 *Data Collection Order* issued by the Wireline Competition Bureau ("Bureau") in the above-captioned proceeding.[2] In the *Data Collection Order*, the Bureau finalized the Federal Communications Commission's ("FCC's" or "Commission's") mandatory special access data collection,[3] which requires providers and purchasers of special access service and certain entities providing "best efforts" business broadband Internet access service to submit data, information, and documents for a comprehensive evaluation of competition in the special access marketplace.

---

[1] *In the Matter of Special Access for Price Cap Local Exchange Carriers*, WC Docket No. 05-25, Application for Review of the National Cable & Telecommunications Association (filed Dec. 9, 2013) ("NCTA Application").

[2] *In the Matter of Special Access for Price Cap Local Exchange Carriers*; *AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Report and Order, DA 13-1909 (rel. Sept. 18, 2013) ("*Data Collection Order"*).

[3] *See In the Matter of Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 16318 (2012) ("*2012 Special Access Order*").

INTRODUCTION AND SUMMARY

NCTA seeks review of the *Data Collection Order*, arguing that the Bureau failed to amend the data collection based on feedback received through the Paperwork Reduction Act ("PRA") process. NCTA also argues that the Bureau ignored critical concerns regarding the security of network maps and detailed customer proprietary network information ("CPNI") sought in connection with the data collection that must be addressed before affected parties can reasonably be expected to submit such information.

While NCTA raises valid concerns regarding both the burden associated with the special access data collection and the potential lack of security measures to protect highly sensitive data requested by the Commission, ITTA urges the Commission to be guided by principles of regulatory parity, practicality, and fairness in reviewing such concerns.

I. ANY MODIFICATIONS TO THE SPECIAL ACCESS DATA COLLECTION MUST BE GUIDED BY PRINCIPLES OF REGULATORY PARITY, PRACTICALITY, AND FAIRNESS

The mandatory data request requires submission of a vast array of data, information, and documents regarding market structure (*e.g.*, the location and type of facilities capable of providing special access and the proximity of such facilities to sources of demand), pricing, demand (*i.e.*, observed sales and purchases), information on terms and conditions in special access contracts, and decision data (*e.g.*, detailed information regarding recent successful and unsuccessful RFPs).[4]

Some of the information required, such as network maps and CPNI relating to every commercial customer to whom providers sell dedicated services, is highly sensitive in nature. Specifically, incumbent providers must disclose the actual situs address (*i.e.*, land where the

[4] *See id*. at ¶¶ 30-46.

building or cell site is located), including latitude and longitude coordinates, for each location to which they provide special access service.[5] Competitive providers must submit highly detailed maps identifying fiber routes and node locations as well as information on the date each node was placed in service.[6] Respondents also must submit detailed CPNI as part of the data collection, given that the *Data Collection Order* now requires disclosure of the customer's name along with detailed information on the type, configuration, location, and quantity of service that the customer receives.[7]

The Commission has, without a doubt, drastically underestimated the amount of time it will take for all respondents to comply with the mandatory special access data collection. As ITTA previously pointed out, compliance will require its members and other respondents to devote thousands of hours to gathering the requested data while diverting internal company resources away from other important functions in areas such as network improvement and optimization, carrier services, toll fraud, billing, and systems integration.[8] In many cases, respondents have not previously been required to comply with recordkeeping or reporting obligations with respect to the data now being requested, so gathering, creating, compiling, and submitting the requested information will require a substantial effort and time commitment from employees in addition to the other roles and functions they are expected to perform within their companies.

That said, ITTA takes issue with NCTA's characterization that the data collection "punishes the very companies that are investing private capital to finally bring widespread

[5] *See Data Collection Order* at Appendix A, § II.B.3.

[6] *Id.* at ¶ 35.

[7] *See id.* at Appendix A, Question II.A.12.b.

[8] *See* Paperwork Reduction Act Comments of the Independent Telephone & Telecommunications Alliance, WC Docket No. 05-25, RM-10593 (filed Apr. 15, 2013), at 4-6.

competition to the special access marketplace."[9] To the contrary, it is incumbent providers of special access service, such as ITTA member companies, that bear the brunt of the burden associated with the Commission's request. As the Commission recognized in the *Data Collection Order*, under each category of data and information identified by the Commission for collection, "most of [the data will] be collected from *Providers*."[10]

Therefore, the Commission must be cautious of arguments that it should further "modify the mandatory special access data collection to reduce the burden on cable operator and other competitive providers."[11] The Commission must keep in mind that the purpose of the mandatory data collection is to ensure a "clear picture of all competition in the marketplace."[12] It is imperative that the Commission refrain from eliminating data submission requirements that would undermine its analysis.

The Commission plans to use the data it collects for a one-time, multi-faceted market analysis that, among other things, evaluates "the intensity of competition (or lack thereof)" in the special access marketplace based on "econometrically sound panel regressions" that examine a multitude factors, including availability, pricing, demand, service characteristics, and terms and conditions relating to the provision of dedicated and "best efforts" services.[13] Targeted relief for cable operators or other competing providers would skew this analysis, producing an "incomplete picture of competition in this market… [that is] likely to lead to inappropriate

[9] NCTA Application at 2.

[10] *Data Collection Order* at ¶ 4.

[11] NCTA Application at 15.

[12] *See 2012 Special Access Order* at ¶¶ 16-19.

[13] *See id*. at ¶¶ 68-69.

regulatory intervention."[14]

The Commission must account fully for robust and growing competition, particularly cable-based competition, if it is to conduct a comprehensive examination of the full scope of actual and potential competition in the special access marketplace that allows it to identify triggers indicating that competitive deployment of facilities is feasible in a given market and therefore sufficient to discipline prices. As such, the Commission should view NCTA's request with a healthy amount of skepticism. To the extent that the Commission is inclined to reduce some of the burdens associated with the data collection, it must do so in a manner that promotes regulatory parity, practicality, and fairness for all who must undertake this massive effort.

II. THE DATA COLLECTION MAY SUBJECT THE NATION'S COMMUNICATONS INFRASTRUCURE AND OTHER CRITICAL INFORMATION TO SUBSTANTIAL RISK

NCTA also raises concerns regarding whether the Commission has adequate data security measures in place to protect the sensitive information it will collect as part of the data request.[15] ITTA shares these concerns.

In addition to the new requirement for respondents to provide CPNI relating to customers that purchase special access service, the data collection calls for highly detailed maps of every telecommunications network in the United States. Information of this nature is exceedingly sensitive, making it ripe for misuse by bad actors intent on disrupting the nation's communications networks. Given the paramount importance of making sure that such information does not fall into the wrong hands, the Commission must ensure that it has policies and controls in place so that this information is not placed at unnecessary risk of improper

[14] Statement of Commissioner Ajit Pai Regarding Release of the Bureau's *Data Collection Order* (Sept. 18, 2013), at 2.

[15] NCTA Application at 13-15.

disclosure, misuse, or destruction.

It is not apparent that the FCC has allocated resources for efficient and effective management and use of the information collected. In particular, there is a clear national security risk if the network mapping data is not managed and stored properly. Given the GAO's findings earlier this year that the FCC needs to "more effectively implement its IT security policies and improve its project management practices," the Commission must ensure that the data being collected is secure against cyber security threats.[16]

In this age of cyber security issues and attacks, protecting sensitive information is of the utmost concern. Cyber-based threats to federal information systems continue to grow and can come from a variety of sources, including criminals, foreign nations, terrorists, and other adversarial groups.[17] Absent adequate safeguards, "systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks."[18]

Obviously, highly detailed maps of every telecommunications network in the United States "would be a target for hackers and others who might be intent on disrupting

---

[16] Government Accountability Office, Information Security, *Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project*, Report No. GAO 13-155 (rel. Jan. 2013), at 20 ("GAO Report"). In examining whether the FCC instituted adequate security measures following a data breach, the GAO Report concluded that the "FCC did not effectively implement appropriate information security controls in the initial components of the ESN project. . . . As a result, FCC limited the effectiveness of its security enhancements and its sensitive information remained at unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction." *Id*. at 9.

[17] *Id.* at 1.

[18] *Id*. at 6.

communications services in the United States."[19] Unauthorized access to the detailed CPNI the Commission now requires respondents to submit also could have harmful consequences. In light of GAO's findings that the FCC has not implemented appropriate information security controls "to sufficiently protect the confidentiality, integrity, and availability of its sensitive information," the Commission must take steps to improve its cyber security practices and ensure that such data is not put at "unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction."[20]

CONCLUSION

In sum, NCTA raises valid concerns regarding both the burden associated with the special access data collection on all respondents and the potential lack of security measures to protect highly sensitive data requested by the Commission. However, ITTA urges the Commission to be guided by principles of regulatory parity, practicality, and fairness in its review of such concerns, and urges the Commission to take steps to ensure the security of the sensitive data it has requested from cyber attacks.

Respectfully submitted,

By: /s/ Genevieve Morelli

Genevieve Morelli
Micah M. Caldwell
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, D.C. 20005
(202) 898-1520
gmorelli@itta.us
mcaldwell@itta.us

December 24, 2013

[19] *See* Letter from Steven F. Morris, NCTA, to Marlene H. Dortch, FCC, WC Docket No. 05-25 (filed Feb. 28, 2013).

[20] GAO Report at 9.