**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** |
| | ) | |
| | ) | |
| **AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services** | ) | **RM-10593** |
| | ) | |
| | ) | |
| **Comprehensive Market Data Collection for Interstate Special Access Services** | ) | **OMB Control No. 3060–XXXX** |

## PAPERWORK REDUCTION ACT COMMENTS OF THE INDEPENDENT TELEPHONE & TELECOMMUNICATIONS ALLIANCE

The Independent Telephone & Telecommunications Alliance ("ITTA") hereby responds to the Commission's request for comment[1] on whether the information collection obligations associated with the mandatory special access data request that the Commission adopted in the above-captioned proceeding[2] satisfy the requirements of the Paperwork Reduction Act of 1995 ("PRA").[3]

---

[1] *Information Collection(s) Being Submitted for Review and Approval to the Office of Management and Budget (OMB)*, Federal Communications Commission, Notice; Request for Comments, 78 Fed. Reg. 73861-73862 (Dec. 9, 2013) ("*PRA Notice*").

[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 and Further Notice of Proposed Rulemaking, FCC 12-153, 27 FCC Rcd 16318 (rel. Dec. 18, 2012) ("*2012 Special Access Order*"), *as modified by 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* Paperwork Reduction Act, Pub. L. 104-13, 109 Stat. 163 (1995), *codified at* 44 U.S.C. §§ 3501-3520.

ITTA is concerned that the Commission has underestimated the amount of time associated with responding to the data request. In fact, compliance with the extraordinarily detailed request would divert substantial resources and take far more time than the Commission acknowledges. Thus, the data request is inconsistent with the policies underlying the PRA, which Congress enacted to "have Federal agencies become more responsible and publicly accountable for *reducing* the burden of Federal paperwork on the public."[4]

ITTA also is concerned that the Commission's information management practices may not be adequate to protect the highly sensitive data it has requested, which includes detailed network maps that would provide the exact location of the nation's telecommunications infrastructure, against cyber security threats. 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 disclosure, misuse, or destruction.

## DISCUSSION

### I. THE COMMISSION'S AUTHORITY IS LIMITED BY THE PRA

The Commission issued the mandatory data collection to obtain comprehensive information on dedicated services that will enable "a robust analysis" and evaluation of competition in the market for special access services.[5] This comprehensive review is intended to aid the Commission in ensuring that its special access rules "reflect the state of competition today and promote competition, investment, and access to dedicated communications services [that] businesses across the country rely on every day to deliver their products and services to

[4] *Id*. at 163 (emphasis added).

[5] *2012 Special Access Order* at ¶ 30.

American consumers."[6] The data request requires the 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).[7]

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 building or cell site is located), including latitude and longitude coordinates, for each location to which they provide special access service.[8] 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.[9] 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.[10] The exceedingly sensitive nature of such data renders it ripe for misuse by bad actors.

While much of the requested information may be useful to the Commission in assessing the market for special access services, the Commission does not have unlimited authority to impose paperwork burdens on providers and purchasers of special access services. Where a

---

[6] *Id*. at ¶ 1.

[7] *See id*. at ¶¶ 30-46.

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

[9] *Id.* at ¶ 35.

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

federal agency seeks to collect information from the public, the PRA mandates that the process minimize the paperwork burden on regulated entities while limiting the cost incurred in collecting, using, and maintaining the information at issue.[11] Accordingly, the PRA requires the Commission to certify to the Office of Management and Budget ("OMB") that, *inter alia*, a proposed information collection:

- "is necessary for the proper performance of the functions of the agency, including that the information has practical utility;"[12]
- "reduces to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency;"[13] and
- "is to be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and record keeping practices of those who are to respond."[14]

The Commission cannot certify compliance with these requirements if it hasn't even completed the threshold step of developing a realistic estimate of the total time required to comply with the proposed data collection.

## II. THE COMMISSION'S PRA ANALYSIS IS FLAWED

The Commission has drastically underestimated the amount of time it will take for respondents to comply with the data collection. The FCC suggests that, on average, respondents will devote 146 hours (18.25 work days) to the mandatory data request.[15] While this figure is intended as an average for all respondents, it grossly underestimates the amount of time required to satisfy the data collection, particularly for larger operators. It also fails to take into account that the burden differs substantially based on the class of respondent. Incumbent providers of

[11] *See* 44 U.S.C. §§ 3501(1), (5).

[12] *Id*. at § 3506(c)(3)(A).

[13] *Id*. at § 3506(c)(3)(C).

[14] *Id*. at § 3506(c)(3)(E).

[15] *PRA Notice* at 73861.

special access service, such as ITTA member companies, 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*."[16]

As CenturyLink stated in response to an FCC inquiry early last year, the estimated burden in terms of the amount of time necessary for the company to comply with the data request will be about 40,000 hours.[17] Consolidated Communications estimates that it will take 10,000 hours for it to gather and report the necessary data. Cincinnati Bell estimates that compliance with the data request will take the company's impacted affiliates nearly 8,000 hours to complete.[18] FairPoint estimates that it will take more than 12,000 hours to complete the data request over a minimum period of six months. This enormous task could take even longer if it occurs during the same timeframe in which FairPoint's subject matter experts are engaged in preparing FairPoint's annual tariff filing.

While other ITTA members are still grappling with the amount of time that will be required to formulate a response to the data request, it is clear that collecting the requested data will require significant efforts by personnel at all affected companies. Employees will have to be redeployed from their regular duties to undertake a number of tasks in connection with responding to the data request, resulting in opportunity costs and loss of productivity due to increased demands on company resources.

For instance, ITTA member companies predict that diverting employees away from their current duties to focus on the data request will come at the expense of other important

[16] *Data Collection Order* at ¶ 4.

[17] *See* Letter from Melissa Newman, CenturyLink, to Marlene H. Dortch, FCC, WC Docket No. 05-25 (filed Jan. 10, 2013).

[18] Comments of Cincinnati Bell Inc., WC Docket No. 05-25 (filed Apr. 19, 2013), at 5.

responsibilities, including in the areas of network improvements (deploying DSLAMs further into the network to increase both speed and availability); network optimization (reviewing network costs and benefits and implementing changes to increase efficiency); carrier services (responding to carrier questions related to circuit operations, such as where particular circuits originate and terminate and on what facilities they ride, which is helpful to carriers who are trying to optimize networks they obtained through mergers and acquisitions); toll fraud (monitoring network usage for toll fraud); and systems integration (meeting internal deadlines for integration projects associated with industry transactions as expected within the investment community). It should be noted that responding to the Data Request also comes at the same time that ITTA members and other providers are continuing to expend substantial efforts to implement the myriad changes the FCC adopted in the *USF/ICC Transformation Order*, which further stretches limited resources.[19]

In addition, a significant amount of time and energy will be devoted to the determination of whether each element of the requested data exists or will need to be created. 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, and compiling 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

[19] *In the Matter of Connect America Fund; A National Broadband Plan for Our Future; Establishing Just and Reasonable Rates for Local Exchange Carriers; High-Cost Universal Service Support; Developing a Unified Intercarrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up; Universal Service Reform – Mobility Fund*, WC Docket Nos. 10-90, 07-135, 05-337, 03-109; CC Docket Nos. 01-92, 96-45; GN Docket No. 09-51, WT Docket No. 10-208, Report and Order and Further Notice of Proposed Rulemaking, FCC 11-161 (rel. Nov. 18, 2011).

companies.[20] It also could significantly add to the amount of time required for submitting a response should respondents need to put systems and/or capabilities in place to present the information in the requested format.

Based on the sheer magnitude of the data request and the impact it will have on the internal resources and operations of respondents, it is clear that the FCC has significantly underestimated the amount of time associated with responding. The Commission's PRA analysis does not properly reflect the scope of the data collection, and therefore is inconsistent with the principles underlying the PRA to minimize the paperwork burden on regulated entities while limiting the cost incurred in collecting, using, and maintaining the information requested.

## III. THE COMMISSION MUST ENSURE IT HAS ADEQUATE SECURITY MEASURES IN PLACE TO PROTECT THE HIGHLY SENSITIVE DATA BEING REQUESTED

Finally, the Commission must ensure that the data it collects is not at risk of cyber security attacks. As indicated above, the data collection calls for highly granular data on the exact location of the nation's telecommunications infrastructure as well as detailed CPNI relating to customers that purchase special access service. Information of this nature is exceedingly sensitive, making it ripe for misuse by bad actors. 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 disclosure, misuse, or destruction.

[20] Many providers and purchasers of dedicated services may only maintain current information with respect to certain data that has been requested, such as fiber maps, geocoded latitude and longitude data for customer locations, and information on nodes between the end user location and the end point of a circuit. Such data may not be available as far back as 2010. Thus, it is important for the Commission to make clear that respondents will not be expected to provide material that they do not possess or that they cannot easily compile and that it will honor respondents' good faith compliance efforts.

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 last 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.[21]

In this age of cyber security issues and attacks, protecting such information is critical. 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.[22] 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."[23]

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 communications services in the United States."[24] 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

[21] 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.

[22] *Id.* at 1.

[23] *Id*. at 6.

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

"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."[25]

## CONCLUSION

In sum, ITTA believes that the Commission has underestimated the amount of time it will take for respondents to comply with the data request, and urges the Commission to ensure that it has adequate information management practices in place to protect the highly sensitive data it has requested. Given the Commission's duty to certify that its information collection activities reduce the burdens on the entities it regulates to the maximum extent possible, the Commission must give further consideration to the actual burden imposed by its comprehensive special access data request, and respond accordingly. Moreover, the Commission must ensure that any data it collects in connection with the request remains secure from improper misuse, disclosure, or destruction through 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

January 8, 2014

[25] GAO Report at 9.