BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of a Working Case to Address Security Practices for Protecting Essential Utility Infrastructure	)))	File No. AW-2015-0206

RESPONSE OF THE MISSOURI CABLE TELECOMMUNICATIONS ASSOCIATION

The Missouri Cable Telecommunications Association (the "MCTA") respectfully opposes the Missouri Public Service Commission Staff's Request for Commission Order (of June 8, 2015) and its Amended Request for Commission Order (of July 17, 2015) to the extent the requests relate to the telecommunications industry.

In its filings, Staff requests the Missouri Public Service Commission (the "Commission") to issue an order requiring several telecommunications-related companies to file written responses to twenty-two (22) questions relating to physical security and cybersecurity issues. Attachment "C" of Staff's Amended Request for Commission Order identified the companies by reference to a list of email addresses.

MCTA is comprised of more than a dozen cable operators and affiliated entities in the telecommunications industry, as well as companies that provide goods or services to telecommunications providers. Several of MCTA's members and their affiliates are certificated by the Commission to provide telecommunications services and were included on "Attachment C" to the Staff's Amended Request for Commission Order.

I. Staff's Request is inconsistent with Staff's Actions and Statements regarding the Scope of this Proceeding

In the Order opening this working case, the Commission noted Staff has filed a Motion in case EW-2013-0011 whereby the **participants in that case have agreed** that the review of security practices should be expanded to include "all utilities." Notably, the only participants in that case were electric utilities. In its Motion to Close Electric Docket and to Open a General Docket filed in Case No. EW-2013-0011, Staff requested that notice be provided to all stakeholders "in the attached list." The attached list only included Missouri regulated electric, natural gas, sewer and water utilities. Telecommunications companies were not part of the "agreement" in EW-2013-011 and the agreement itself only related to electric, natural gas, sewer and water utilities. This is evidenced by the fact that only those utilities were invited to participate in the workshop held on March 23, 2015. At the workshop, the Staff stated that "Electric utilities, Natural gas utilities, Water/Sewer utilities" are the entities "[w]ho should be requested/required to report information related to cybersecurity/physical infrastructure threats."[1]

To MCTA's knowledge, no representatives from the telecommunications industry were notified of, present at, or requested by Staff to attend and/or participate in the Workshop. Staff's attempt to now include the telecommunications industry in this proceeding exceeds the agreement in EW-2013-0011 and the stated scope of this proceeding.

[1] "PSC Presentation – Cybersecurity/Physical Infrastructure Security Workshop – March 23, 2015," slide 9, filed on April 13, 2015).

II. The Federal Communications Commission ("FCC") is Comprehensively Addressing Cybersecurity Issues and the Commission Should Not Engage in Duplicative or Inconsistent Efforts

MCTA agrees with STCG, AT&T and CenturyLink that it is unnecessary to involve telecommunication companies in this proceeding. The FCC is already pursing a comprehensive, national effort to develop best practices for cybersecurity as it relates to the telecommunications industry. With the issuance of the 2013 Presidential Executive Order 13636, "Improving Cybersecurity Critical Infrastructure," and the subsequent 2014 release of the NIST Cybersecurity FrameworkVersion 1.0, there has been renewed emphasis on cybersecurity risk management. More than one hundred professionals and stakeholders worked for more than a year to produce "The Cybersecurity Risk Management and Best Practices Working Group 4: Final Report" in March 2015.[2] The 415-page report covers five industry segments: Broadcast, Cable, Satellite, Wireless, and Wireline, and describes mechanisms that give the FCC and the public assurance that communication providers are taking the necessary measures to manage cybersecurity issues. On March 19, 2015, the FCC issued a Public Notice seeking Comment on the Report as part of its ongoing effort to "develop effective and proactive private sector-driven cyber risk management."[3] Initial comments were submitted May 29, 2015 and reply comments on June 26, 2015. The National Cable & Telecommunications Association has been extensively involved in the federal efforts relating to best practices

[2] Available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.

[3] Available at https://apps.fcc.gov/edocs_public/attachmatch/DA-15-354A1.pdf.

for telecommunications cybersecurity. The effort by the Staff to also address cybersecurity issues in this case would be duplicative, and could result in inconsistent requirements.

III. Staff's Requests Conflict with this Commission's Order in Case No. EW-2013-0011

The Staff asks this Commission to issue an order in conflict with the Commission's previous Order in EW-2013-0011. In opening working docket EW-2013-011, the Commission stated "it must explore, and ensure, the integrity of the **electric** utilities internal cybersecurity practices."[4] In that case, the Commission posited questions to the regulated electric utilities which covered topics of cybersecurity planning, standards, procurement policies, personnel and policies, and systems and operations. The Staff issued a Report which summarized the electric utilities' responses and efforts.[5] On March 13, 2013, the Commission issued the following order in that case:

> **No notifications or reports concerning the matters outlined in Staff's recommendation shall be made in documentary form, i.e. no physical, digital or electronic reports shall be produced or filed in any docket, workshop, investigation or case, either noncontested or contested; nor shall the information provided to Staff be transmitted electronically to Staff or shared with any other entity. The information shall only be reported orally to designated Staff members[.]**

[4] Order Directing Notice and Directing Filing, Case No. EW-2013-0011 (July 17, 2012), p. 3.

[5] Staff Report, Cybersecurity Practices for Protecting Essential Electric Utility Infrastructure, Case No. EW-2013-011 (Feb. 8, 2013).

(Emphasis added and footnote omitted).[6] Here, the Staff is asking the Commission to Order all utilities to report in written form information that the Commission previously ordered shall only be reported "orally." Because Staff's request is inconsistent with the Commission's Order in EW-2013-0011, it should be denied.

The reasoning for the Commission's Order in EW-2013-0011 was highlighted by the Staff at the workshop in this case. First, Staff explained "[i]n cybersecurity, the information itself is sometimes the asset worth stealing."[7] Second, information gathered by the Commission could potentially subject to open records request, making the information publicly accessible.[8] The Staff noted that "many states have good cybersecurity exemption rules"; however, Missouri's open records law (Section 610.021, RSMo) does not appear to contain an exemption that would expressly and unambiguously protect the responses requested by Staff here. Finally, Staff noted even if the information can be shielded from the open records law, it may still be "vulnerable to cyber attack."[9] These reasons mandated the Commission's Order in EW-2013-0011 that cybersecurity information only be reported "orally" and the same reasons justify denying Staff's current request that the Commission order the information be made in documentary form.

---

[6] Order Regarding Staff Recommendation and Motion for a Waiver or Variance, Case No. EW-2013-0011 (March 13, 2013), p. 2.

[7] "PSC Presentation – Cybersecurity/Physical Infrastructure Security Workshop – March 23, 2015," slide 8, filed on April 13, 2015).

[8] *Id.*

[9] *Id.*

WHEREFORE, MCTA respectfully requests that the Commission decline Staff's request to the extent it includes telecommunications service providers; or, in the alternative, issue an order that (a) declares responses to Staff's cybersecurity and critical infrastructure security questions are optional and voluntary for telecommunications companies and (b) designates any response shared by telecommunications companies as highly confidential and protected from public disclosure.

Respectfully submitted,

BLITZ, BARDGETT & DEUTSCH, L.C.

By: /s/ Stephanie S. Bell

Stephanie S. Bell, #61855
308 East High Street, Suite 301
Jefferson City, MO 65101
Telephone No.: (573) 634-2500
Facsimile No.: (573) 634-3358
E-mail: sbell@bbdlc.com

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was sent by email this 31 day of July, 2015, to the parties of record as set out on the official Service List maintained by the Data Center of the Missouri Public Service Commission for this case.

/s/ Stephanie S. Bell