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

COMMENTS OF THE
MISSOURI CABLE TELECOMMUNICATIONS ASSOCIATION

The Missouri Cable Telecommunications Association[1] (the "MCTA") respectfully provides comments in response to the Missouri Public Service Commission's (the "Commission's") June 13, 2017 Notice of Opportunity to Comment ("Notice"), to the extent the requests relate to the telecommunications industry.

In Attachment A of the Notice, and in connection with its scheduled July 11, 2017 Workshop meeting regarding cybersecurity and physical infrastructure, the Commission invites input from stakeholders, including both regulated and unregulated utilities, regarding a series of questions relating to physical security and cybersecurity issues. Specifically, the Notice indicates the goal of the Workshop is to discuss several important issues relating to cyber and physical infrastructure security, including:

- Protections to prevent information disclosure;
- Development and usefulness of security metrics and measures;

[1] 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 the mailing list for the Notice. Participation in this proceeding by MCTA and its member companies does not constitute, nor shall it be deemed to constitute, a waiver, either expressly or implied, by MCTA or its member companies of any constitutional or legal right which each entity has or may be determined to have, including by subsequent legislation or administrative or court decisions. MCTA and its member companies each hereby reserve all of their rights under applicable federal and state constitutions and laws. Nor does MCTA's or its member companies' participation in this proceeding constitute a waiver by them with respect to the State of Missouri's or the Commission's jurisdiction or authority to regulate their cyber security practices or infrastructure security.

- Possible formal or informal methods of information sharing amongst utilities;
- Need for mutual aid agreements between utilities to address cyber/physical security incidents.

This request is a continuation of the inquiry first initiated by the Commission in July 2012 (File No. EW-2013-0011) to address concerns regarding effective cybersecurity practices for protecting essential electric utility infrastructure. Additional developments led to the opening of the instant docket, and the Commission, in its August 5, 2015 Order, directed telecommunications providers to respond to certain specific questions. On October 23, 2015, the Commission's Staff issued a Report recommending no specific reporting requirements for telecommunications providers, while encouraging telecommunications providers to interact with Staff in the event of cybersecurity or physical infrastructure events or breaches that affect many customers, involve the release of proprietary information, or pose a threat to the general public.

MCTA's member companies appreciate the Commission's continued interest in, and commitment to, understanding and reinforcing the importance of developing and maintaining reasonable cybersecurity practices for Missouri's regulated and unregulated utilities. MCTA shares the overall views reflected in legislation enacted by Congress, policy-making by numerous agencies at the Federal level, and the reasoned involvement of state actors and affiliated organizations, like the National Association of Regulatory Utility Commissioners (NARUC), that the most effective means of enhancing our overall cyber defense posture is through a public-private collaborative partnership that emphasizes identification and voluntary adoption of best practices, and ensures flexibility and innovation for companies engaged in securing assets against cyberattacks.

MCTA provides comments as follows:

I. Additional PSC Oversight of Telecommunication Provider Cyber and Infrastructure Security Efforts is Not Necessary at This Time

As a threshold matter, MCTA supports the overall objectives associated with the issues raised by the Notice – to clarify the extent of necessary Commission involvement in cybersecurity and related matters, in light of the high level of federal activity and clear directives in this area. MCTA notes that the scheduled workshop and related activities are a continuation in this docket of the Commission's 2015 examination of almost-identical issues. MCTA filed comments in that phase of the proceeding, urging the Commission to continue its support of meaningful and voluntary efforts taken by telecommunications providers in this area, given the extensive and continuing efforts to establish a national framework of best practices by numerous federal agencies, including the Department of Homeland Security, and given that the "FCC is already pursuing a comprehensive, national effort to develop best practices for cybersecurity as it relates to the telecommunications industry."[2] Consistent with the recommendations of MCTA and other telecommunications providers, the Commission Staff's October 23, 2015 Report made clear that since "utilities are [already] actively engaged in cybersecurity and infrastructure security issues, Staff does not recommend the Commission promulgate rules related to cybersecurity or infrastructure security" (Pg.7). Specifically with regard to telecommunications providers such as MCTA's members' affiliates, the Staff Report also explained that:

> Due to limited jurisdiction over telecommunications providers, Staff does not recommend any changes to the process at this time. Staff recommends the Commission encourage telecommunications providers to interact with Staff in the event there are cybersecurity or infrastructure security events or breaches that affect many customers, the release of customer proprietary information or pose a threat to the general public (Pg. 6).

MCTA respectfully submits that for telecommunications providers and their affiliates, the level of active federal and private sector engagement on cyber and physical infrastructure issues has

[2] Response of the Missouri Cable Telecommunications Association, filed July 31, 2015, p. 3.

only increased since the Commission's 2015 inquiry, obviating any need for overlapping and potentially conflicting state involvement at this time.

II. Federal Agencies Continue to Comprehensively Address Cybersecurity Issues

As the Commission notes in the Notice, there are numerous federal activities currently focusing on improving the nation's ability to combat cyber threats and attacks, including both the continuation of efforts established by the Obama Administration as well as additional mandates initiated by the Trump Administration. Both individually and also via the industry's national advocacy group, The National Cable & Telecommunications Association ("NCTA"), MCTA members remain extensively involved in these federal efforts relating to best practices for telecommunications cybersecurity. Accordingly, efforts by the Commission to also comprehensively address cybersecurity issues in this case would be duplicative, and could result in inconsistent requirements.

Below is a partial list of ongoing federal activities in which MCTA members and/or NCTA, in partnership with the broader communications sector, are actively participating:

1) US Commerce Department: NIST Cybersecurity Framework update
   - National Institute of Standards and Technology issued draft 1.1 framework revising 2014 Cyber Framework
   - Comments filed in April 2017
   - NIST has conducted workshops, which included discussion of metrics, confidentiality and sector interface issues
   - NIST expects to issue its final report Fall 2017

2) White House Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
   - Issued May 2017; calls for Department of Homeland Security and the U.S. Commerce Department to lead process to reduce botnets and improve resilience of the internet and communications ecosystem;
   - Mandates a series of reports from federal agencies over the next year;
   - https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

3) US Commerce Department
   - NTIA - In response to Executive Order, on June 8, 2017 issued Request for Comment on "Promoting Stakeholder Action Against Botnets and Other Automated Threats"
   - Comments are due July 28, 2017; NIST hosting two-day workshop with industry, July 11 – 12, 2017;
   - https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.
   - Draft report expected January 2018; final report May 2018.
   - The Cable sector, along with the broader communication sector, submitted comments, via the Communication Sector Coordinating Council (CSCC) on June 28th.

4) US Commerce Department, Internet Policy Task Force
   - Task Force security paper in development;
   - Comments on draft "green paper" filed in March 2017;
   - White Paper expected before year-end 2017.

5) White House National Security Telecommunications Advisory Committee (NSTAC), an industry advisory group
   - Developing report on botnets, DDOS attacks, IoT as attack vector, etc. and the resiliency of the communications infrastructure
   - Group co-chaired by AT&T and Sonus; report due to President, October 31, 2017.
   - NCTA members providing technical expertise to the committee. Again this is in conjunction with the CSCC.

6) US Department of Homeland Security collaboration with Commerce on botnet initiatives. The Department also has a host of ongoing cyber-related activities, including promoting its automated cyber threat indicator sharing system (AIS), CISCP program, National Security Indicator Exchange (NSIE), and fully supports an Information Sharing and Analysis Center (ISAC) for communications. The Comm-ISAC has been in existence since 2000, operates under a National Security Emergency Preparedness (NS/EP) construct, has 67 industry entities and multiple Federal and State government agencies as members, incorporates a 24/7 watch, provides multiple cyber and physical products daily to its members, conducts weekly meetings with government and industry coming together, acts as a conveyer to bring together Federal and State agencies, and industry members of the Comm-ISAC during both physical and cyber events.

7) FCC – Communications Security, Reliability and Interoperability Council (CSRIC)
   - On June 2017, the Commission launched CSRIC VI and announced formation of a "Network Reliability and Security Risk Reduction" Working Group
   - The Working Group will, among other things, recommend mechanisms to reduce risks to network reliability and security, including best practices to mitigate risks from IoT devices, IP-based networks and protocols, border gateway protocol; domain name server; open-source software platforms used in 5G networks;

wireless platforms. MCTA members will be very involved in this working group.

- https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council.

8) Communications Sector Coordinating Council (CSCC)
   - Group comprised of leading communications companies, works with the Department of Homeland Security as the sector-specific agency for communications.
   - https://www.comms-scc.org/about-1.

Taken together, these ongoing activities at the federal level reflect a comprehensive scheme already in place to address the key metrics, sector coordination and reporting issues implicated in the Commission's Notice. Because of the extensive involvement of MCTA members and other communications providers in these initiatives, overlapping and potentially duplicative state regulation or oversight is not necessary at this time

WHEREFORE, MCTA respectfully recommends that the Commission continue to monitor and support the numerous voluntary initiatives underway by various expert federal agencies to create national guidelines and best practices for telecommunications providers regarding their cyber and physical infrastructure security, but take no further action respecting such providers.

Respectfully submitted,

Andrew B. Blunt
Executive Director
P.O. Box 1185
Jefferson City, MO 65102
(573) 632-4184

Terry M. Jarrett MO Bar 45663
HEALY LAW OFFICES, LLC
514 E. High St., Suite 22
Jefferson City, MO 65101
Telephone: (573) 415-8379
Facsimile: (573) 415-8379
Email: terry@healylawoffices.com

CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing have been mailed, emailed or hand-delivered to all parties on the official service list for this case on this 5th day of July, 2017.

Terry M. Jarrett