BEFORE THE PUBLIC SERVICE COMMISSION OF THE STATE OF MISSOURI

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

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") October 2, 2019 Order Requesting Responses to Staff's Follow-Up Report ("Order"). In the Order, the Commission invites input from interested stakeholders. 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

[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.

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.

This Order 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. The Commission's staff filed a Follow-Up Report on October 2, 2019, which led to the Order to which we are now responding.

To start, MCTA notes the limited jurisdiction that this Commission retains over telecommunications providers. *See Follow-Up Report § 4.1(2)(ii)*. Given that limited jurisdiction, the Follow-Up Report quite properly recommends that the Commission "encourage" interaction between telecommunications providers and Commission staff, but does not impose a mandate.

Second, MCTA supports the overall objectives associated with the issues raised by the Follow-Up Report – 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 various FCC working groups. MCTA also filed comments on July 7, 2017. As the 2019 Follow-Up Report and previous PSC workshops and reports acknowledge, the most effective approach is bolstering cybersecurity utilities companies to be agile, flexible and forward-looking. Because prescriptive measures are generally backward-looking and static, they tend to be ill-suited for strengthening overall cybersecurity.

Third, MCTA wants to bring to the attention of the Commission the many federal limitations in the cyber security area. As the 2019 Follow-Up Report acknowledges, overlapping and conflicting cyber oversight mechanisms, however well-intentioned, undermine the objective of augmenting utility cyber defenses. Before imposing any additional oversight or reporting mechanisms, the PSC should be fully mindful of the wide range of existing initiatives ongoing at the Federal level, including:

NIST Cybersecurity Framework v.1.1. In April 2018, the National Institute for Standards and Technology (NIST) completed its 15-month long process of updating its 2014 Cybersecurity Framework by releasing the final Version 1.1 of the Framework. Version 1.1 reaffirmed the primacy of voluntary measures to address cybersecurity readiness, included new guidance on self-assessment and metrics to aid companies in gauging their internal progress managing cyber risks, and added a new section on supply chain risks management to help organizations identify, assess, and mitigate potential malicious functionality or vulnerabilities in technology-related products so that the procurement process helps organizations meet key security outcomes.

White House Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The May 2017 Executive Order provided the foundation for a considerable amount of recent Federal cyber policy activity, including the following:

- Comprehensive review to strengthen resilience of "the Internet and communications ecosystem" against DDOS attacks, botnets, and other cyber threats, resulting in the May 2018 release of the Botnet Report.
- New SEC guidance to promote appropriate market transparency of cyber risk management practices
- Continued focus on support for owners and operators of critical infrastructure "at greatest risk"

- Additional efforts to improve the cybersecurity practices of federal agencies, including a directive to each agency head to use the NIST Cybersecurity Framework to manage cybersecurity risk

Administration Botnet Report. In May 2018, DHS and the Commerce Department's National Telecommunications and Information Administration (NTIA) issued "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats." The Report highlighted the "interdependence" of the Internet and digital services ecosystem, noting that due to "the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem, no single tool can secure the infrastructure." It also stressed the need for baseline security profiles for IoT devices and improvements in software development, patching, and upgrading, and emphasized that the global nature of the problem requires coordination with international partners. The Administration's November 2018 Road Map outlines a prioritized and sequenced plan for various government and private sector stakeholders to implement the key recommendations of the Botnet Report.

DHS Information Sharing Initiatives. 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 and other industry sectors. The Comm-ISAC has been in existence since 2000, operates under a National Security Emergency Preparedness (NS/EP) construct, has 70 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, and acts as a conveyer to bring together Federal and State agencies, and industry members of the Comm-ISAC during both physical and cyber events.

Federal Supply Chain Risk Management Initiatives. There are multiple Federal work streams addressing supply chain issues, including the following:

- Implementation of section 889 of the 2019 National Defense Authorization Act, which imposed agency procurement/contracting restrictions on equipment from Huawei, ZTE, and a handful of foreign video surveillance equipment - and authorized DoD to add additional entities to the list;
- The new authorities afforded to the Commerce Department by the May 2019 Executive Order on the Information and Communications Technology (ICT) supply chain;
- The ongoing information technology and communications sector supply chain risk assessment taking place at DHS under the aegis of the National Resource Management Center and in conjunction with the activities of the ICT Supply Chain Task Force;
- The NIST guidance on supply chain risk management in the NIST Cybersecurity Framework; and

- The FCC proceeding on restricting universal service support for companies that use prohibited equipment posing a national security risk.

FCC – Communications Security, Reliability and Interoperability Council (CSRIC). In March 2019, the CSRIC VI Network Reliability and Security Risk Reduction Working Group released its final report on "Best Practices and Recommendations to Mitigate Security Risks to Current IP-Based Protocols." The report 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; and wireless platforms. MCTA members were actively involved in this working group.

In addition to the above, the Department of Commerce's National Institute for Standards and Technology (NIST) has several ongoing cybersecurity-related activities, notably mitigating risks from IoT devices. In June 2019, it issued a publication on Managing Internet of Things Cybersecurity and Privacy Risks. Also, the National Telecommunications and Information Administration (NTIA) is conducting a multi-stakeholder process with industry experts focused on software component transparency to foster better security decisions and practices.

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,

By: */s/ Andrew B. Blunt*
Andrew B. Blunt
Executive Director
MCTA
P.O. Box 1185
Jefferson City, MO 65102
573-680-6966
ablunt@hbstrategies.us