STATE OF MISSOURI
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held at its office in Jefferson City on the 5th day of July, 2015.

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

ORDER DIRECTING UTILITIES TO RESPOND TO QUESTIONS ABOUT SECURITY PRACTICES FOR PROTECTING ESSENTIAL UTILITY INFRASTRUCTURE

Issue Date: August 5, 2015 Effective Date: August 15, 2015

The Commission opened this working case on March 4, 2015, to address concerns about physical and cybersecurity practices to protect essential utility infrastructure. A workshop regarding those concerns was conducted on March 23, and the consensus among participants was that the Commission's Staff should, in consultation with other stakeholders, develop a set of questions to be sent to all Missouri utilities to help assess how effectively those utilities are dealing with security issues.

Staff developed a list of questions, and filed a motion asking the Commission to send those questions to the utilities. Staff amended that request on July 17. The Missouri Small Telephone Company Group, the Missouri Independent Telephone Company Group, the Missouri Cable Telecommunications Association, AT&T, and CenturyLink filed responses to Staff's amended request. The telecommunications companies ask the Commission to exempt them from Staff's request for information, arguing that because they are subject to the FCC's security regulations, it would be

inconsistent and burdensome for them to answer Staff's questions in this proceeding. After further discussions, Staff and some of the concerned telecommunications companies have reached a compromise whereby the telecommunications companies have agreed to voluntarily answer a shortened list of questions.

The following are the questions to which each non-telecommunications utility shall respond:

1. Does your company participate in an internal or external critical infrastructure or cybersecurity vulnerability assessment? If yes,
    a. Is the assessment conducted by a qualified independent third party and if so, by whom?
2. If your company has deployed Advanced Metering Infrastructure (AMI), does your company have independent security audits conducted on a periodic basis?
3. Does your company have a written policy regarding the treatment of customer data?
    a. Is the written policy regarding treatment of customer data shared with your customers?
    b. Does your process or policy include associated timeframes for notifying customers if a successful cybersecurity breach occurs that impacts customer data?
4. Please provide an organizational diagram of the company's security team, including all required support personnel
5. Does the company have a qualified security team with adequate support personnel?
6. Does your company participate in regional or national tabletop exercises, conferences, committees or other events related to critical infrastructure security threats and/or cybersecurity threats? If yes, please identify the various groups, activities or events.
7. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to critical infrastructure security threats? If yes,
    a. Does your plan include alternative methods for meeting critical functions in the event of an incident?
    b. Does your company have retainers or contracts for outside help in the event of an incident?
    c. Does your company participate in any resource sharing agreements or mutual assistance agreements?

8. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to cybersecurity threats?
    a. Does your plan include alternative methods for meeting critical functions (continuity of operations plans and disaster recovery plans) in the event of an incident?
9. Has your company conducted a physical and logical security evaluation of key assets in concert with federal guidelines?
10. Has your company conducted a cybersecurity or physical security risk assessment?
11. Does your company have retainers or contracts for outside help in the event of an incident?
12. Does your company participate in any resource sharing agreements or mutual assistance agreements?
13. Does your company have a process in place to alert of threats to critical infrastructures?
14. Does the company employ risk or vulnerability assessment tools that relate to critical infrastructure security or cybersecurity?
15. Does your company keep records of attempted or successful threats to critical infrastructure or cybersecurity?
16. Does the company have a reporting process in the event of an attempted breach of critical infrastructure, whether successful or not?
17. Does your company have an internal root cause analysis and correction action process to evaluate critical infrastructure security and to take action to prevent an event and/or recurrence?
18. Does the company have a reporting process in the event of an attempted cybersecurity breach, whether successful or not?
19. Does the company have a reporting process if a successful cybersecurity breach does occur that impacts customer data?
20. Does your company have an internal root cause analysis and correction action process to evaluate cybersecurity and to take action to prevent an event and/or recurrence?
21. What interaction/reporting, if any, should occur between your company and the Missouri Public Service Commission related to critical infrastructure security or cybersecurity?
22. What format should be used to provide the interaction/reporting described in response to question 21?

The Commission asks the telecommunications utilities to respond to the following questions:

1. Does your company have a written policy regarding the treatment of customer data?

   a. Does your process or policy include associated timeframes for notifying customers if a successful cybersecurity breach occurs that impacts customer data?
2. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to critical infrastructure security threats? If yes,
   b. Does your plan include alternative methods for meeting critical functions in the event of an incident?
3. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to cybersecurity threats?
   a. Does your plan include alternative methods for meeting critical functions (continuity of operations plans and disaster recovery plans) in the event of an incident?
4. Has your company conducted a cybersecurity or physical security risk assessment?
5. What interaction/reporting, if any, should occur between your company and the Missouri Public Service Commission related to critical infrastructure security or cybersecurity?
6. What format should be used to provide the interaction/reporting described in response to question 5?

Each response shall name the utility responding, and shall identify a contact person at that utility, including information about how to contact that person.

THE COMMISSION ORDERS THAT:

1. The Commission's Data Center shall provide a copy of this order to the organizations and persons identified on attachments B and C to Staff's motion. The Data Center shall also provide a copy of this order to all incumbent local exchange telecommunications companies providing service in Missouri.

2. The utilities receiving this order may respond to the questions listed in this order by submitting a response to Staff by sending a paper response to Natelle Dietrich, or by responding electronically at natelle.dietrich@psc.mo.gov no later than September 11, 2015. Responses should not be filed in the Commission's electronic filing and information system, EFIS.

3. The utilities receiving this order may submit their response to the questions as a highly confidential or proprietary document if they wish to do so.

4. This order shall be effective on August 15, 2015.

BY THE COMMISSION

Morris L. Woodruff
Secretary

Kenney, Chm., Stoll, W. Kenney,
Hall, and Rupp, CC., concur.

Woodruff, Chief Regulatory Law Judge