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**

STAFF REPORT

COMES NOW the Staff of the Missouri Public Service Commission ("Staff"), through the undersigned counsel, and respectfully states as follows:

On March 4, 2015, the Commission issued an Order that opened this matter to include all utilities and include cybersecurity as well as physical infrastructure security. Subsequently, the Staff held a workshop and inquired of utilities about their security plans and procedures. The attached Staff Report summarizes the Staff's findings and includes its recommendations.

WHEREFORE, the Staff submits its Report.

Respectfully submitted,

Colleen M. Dale
Senior Counsel
Missouri Bar No. 31624
Attorney for the Staff of the
Missouri Public Service Commission
P. O. Box 360
Jefferson City, MO 65102
(573) 751-4255 (Telephone)
cully.dale@psc.mo.gov

CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing have been mailed, hand-delivered, transmitted by facsimile or electronically mailed to all counsel of record this 23rd day of October, 2015.

MEMORANDUM

To: Missouri Public Service Commission Official Case File
File No. AW-2015-0206

From: Natelle Dietrich 10/23/15
Staff Director/Date

Colleen M. Dale 10/23/15
Senior Counsel/Date

Background

In July 2012, the Commission opened a working case, File No. EW-2013-0011, to address concerns about effective cybersecurity practices for protecting essential electric utility infrastructure. On February 19, 2015, Staff filed a motion in that case asking the Commission to close that working docket and open a new expanded working case to include all utilities and to include physical security threats as well as cybersecurity threats. The present case was opened on March 4, 2015. A workshop was held on March 23, 2015 to discuss issues related to cybersecurity and physical infrastructure security. On June 8, 2015 and July 17, 2015, Staff filed requests asking the Commission to direct utilities to respond to a number of questions related to infrastructure and cybersecurity. On August 5, 2015, the Commission issued an order directing utilities to respond to the following questions by September 11, 2015. Telecommunications providers were directed to respond to a subset of the questions. Highly confidential responses were received via EFIS, email and hard copy.

High Level Summary of Responses

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?**

Non-telecommunications: All responders indicated they participate in vulnerability assessments.

2. **If your company has deployed Advanced Metering Infrastructure (AMI), does your company have independent security audits conducted on a periodic basis?**

Non-telecommunications: Most responders indicated they do not deploy AMI.

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 which impacts customer data?**

Non-telecommunications: Responders indicated they have a written policy. Some responders indicate they do not have specific timeframes for notifying customers. Others indicate they follow state and federal requirements for notifying customers.

Telecommunications: Responders indicated they have a written policy and follow applicable FCC rules, state laws or data breach laws.

4. **Please provide an organizational diagram of the company's security team, including all required support personnel.**

Non-telecommunications: Responders provided information responsive to this question.

5. **Does the company have a qualified security team with adequate support personnel?**

Non-telecommunications: Responders indicated they have qualified security teams 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.**

Non-telecommunications: Responders provided various groups, activities and events in which they participate.

7. **Does your company have emergency preparedness plan(s) that include policies and procedures that includes 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 of mutual assistance agreements?**

Non-telecommunications: Responders have emergency prepared plans that meet the parameters set forth in the question. Not all responders have retainers or contracts for outside help.

Telecommunications: Responders comply with PSC rules on emergency prepared plans.

8. **Does your company have emergency preparedness plan(s) that include policies and procedures that includes 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?**

Non-telecommunications: Responders have emergency prepared plans that meet the parameters set forth in the question.

Telecommunications: Responders either have emergency preparedness plans in place to address cybersecurity threats or are monitoring the FCC's docket on cybersecurity.

9. **Has your company conducted a physical and logical security evaluation of key assets in concert with federal guidelines?**

Non-telecommunications: Responders indicate they have conducted physical and logical security evaluations and follow applicable Department of Energy and National Institute of Standards and Technology (NIST) models and standards.

10. **Has your company conducted a cybersecurity or physical security risk assessment?**

Non-telecommunications: Responders have conducted risk assessments.

Telecommunications: Some responders have conducted risk assessments.

11. **Does your company have retainers or contracts for outside help in the event of an incident?**

Non-telecommunications: Some responders have retainers or contracts for outside help.

12. **Does your company participate in any resource sharing agreements or mutual assistance agreements?**

Non-telecommunications: Most responders have sharing agreements or mutual assistance agreements.

13. **Does your company have a process in place to alert of threats to critical infrastructures?**

Non-telecommunications: Responders have a process in place.

14. **Does the company employ risk or vulnerability assessment tools that relate to critical infrastructure security or cybersecurity?**

Non-telecommunications: Responders employ risk or vulnerability assessment tools.

15. **Does your company keep records of attempted or successful threats to critical infrastructure or cybersecurity?**

Non-telecommunications: Responders maintain records as outlined in the question.

16. **Does the company have a reporting process in the event of an attempted breach of critical infrastructure, whether successful or not?**

Non-telecommunications: Responders have a reporting process consistent with the question.

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?**

Non-telecommunications: Most responders indicate they have an internal root cause analysis and correction action process related to infrastructure security.

18. **Does the company have a reporting process in the event of an attempted cybersecurity breach, whether successful or not?**

Non-telecommunications: Responders have a reporting process as outlined in the question.

19. **Does the company have a reporting process if a successful cybersecurity breach does occur that impacts customer data?**

Non-telecommunications: Responders have a reporting process as outlined in the question.

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?**

Non-telecommunications: Responders indicate they have an internal root cause analysis and correction action process related to cybersecurity.

21. **What interaction/reporting, if any, should occur between your company and the Missouri Public Service Commission related to critical infrastructure security or cybersecurity?**

Non-telecommunications: Responses included -

- Use Commission reporting requirements under 4 CSR 240-3.190 for cybersecurity and physical security threats
- Use verbal reporting of events or incidents
    - Should be considered highly confidential
    - Could include type of incident, date and time
- Provide annual updates to the 20 cyber/infrastructure security questions
- Maintain key stakeholder contact and regular communications about issues impacting the state's critical infrastructure.

Telecommunications: Responses included –

- File disaster recovery plans with Commission
- Make cybersecurity plans available upon request

- Not necessary to report, but happy to discuss ad hoc issues
- Should only have to report outages consistent with Commission rules
- Should be a unified national approach to reporting
- To the extent the Commission would like information, it should follow FCC rules/activities
- Commission should have a representative on the Missouri Information Analysis Center (MIAC)

22. What format should be used to provide the interaction/reporting described in response to question 21?

Non-telecommunications: Responses included –

- Use Commission reporting requirements under 4 CSR 240-3.190 for cybersecurity and physical security threats major events
- Verbal reporting
    - Highly confidential
    - Not disclosed to others
    - Phone call
    - Face-to-face meeting with key stakeholders
- Conference calls as needed

Telecommunications: Responses included –

- Verbal communication with Staff.
- No electronic or written documentation
- Communication with Commission/Staff not necessary
- Respond to general questions via email
- Communications should only be real-time if events occur
- Email, phone, texts, in-person, hand-delivered as conditions warrant

Summary and Staff Recommendation

Questions 1-20 – General infrastructure and cybersecurity issues

It appears from the responses that, for the most part, Missouri utilities have taken a proactive role in cybersecurity and infrastructure security preparedness. The few questions where utilities responded "no", the lack of action is due to the size of the utility, limitations on technology or the monitoring of federal action on related activities. **Since the utilities are actively engaged in cybersecurity and infrastructure security issues, Staff does not recommend the Commission promulgate rules related cybersecurity or infrastructure security.**

Questions 21 and 22 – Reporting to the Commission

All utilities indicated a degree of willingness to keep the Commission informed on cybersecurity and infrastructure security issues. However, most utilities indicated a preference for either verbal reporting of events or no reporting of events. In Staff's opinion, it is appropriate for the Commission to have information related to the safety and security of the utilities it regulates. Processes are currently in place for communications from natural gas and electric utilities to report incidents or events that result in injury, death, significant infrastructure damage, or may

result in significant attention (i.e., make sure the Commission is aware of an incident before it learns about it through the news).

Staff Recommendation

Non-telecommunications: Staff recommends this process be expanded for all non-telecommunications utilities to include verbal reporting of cybersecurity or infrastructure security events or breaches that affect many customers, involve the release of customer proprietary information or pose a threat to the general public.[1] Reports will be provided to a Staff member directly involved with emergency management functions.[2] Staff will verbally inform the Chairman/Commissioners as deemed appropriate. While written records will not be retained regarding individual contacts, the information may result in Staff or the Commission requesting an investigation into any potential larger issues.

Telecommunications: 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.

[1] As with the reporting of events that may receive large public attention, this may result in a judgement call on the part of the utility as opposed to establishing a bright line.

[2] Staff Director (Natelle Dietrich), Manager Engineering Analysis (Dan Beck), Manager Safety Engineering Unit (Bob Leonberger) or Manager Water and Sewer Unit (Jim Busch)