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	)))	**Case No. AW-2015-0206**

NOTICE OF OPPORTUNITY TO COMMENT

Issued: June 13, 2017

The Commission has invited stakeholders to participate in a workshop meeting regarding cybersecurity and physical infrastructure security to be held on July 11, 2017. On June 6, Staff filed a list of topics and questions that it intends to address at the workshop meeting. The Commission will invite interested stakeholders to address the following topics and questions identified by Staff in the attached document. Staff asks that stakeholders file their comments in this file by July 5, 2017.

BY THE COMMISSION

Morris L. Woodruff
Secretary

Morris L. Woodruff, Chief Regulatory Law Judge, by delegation of authority pursuant to Section 386.240, RSMo 2016.

Dated at Jefferson City, Missouri, on this 13th day of June, 2017.

ATTACHMENT A

I. Intended Audience, Participants, and Goals

The intention of this workshop is to bring together the Public Service Commission (PSC) with representatives of both regulated and unregulated utilities (investor owned, cooperative, and municipal, electric, natural gas, water, sewer, and telecommunications utilities), trade groups, industry associations, and other state agencies to discuss cyber and physical security issues with the following goals:

- Examine protections available or still necessary to prevent disclosure of information related to cyber and physical security of critical infrastructure.
- The development of cyber and physical security measures and metrics, and the potential usefulness of reporting such measures and metrics.
- The development of a method (formal or informal) of information sharing amongst Missouri utilities related to cyber and physical security.
- The development of mutual aid agreements between utilities in reference to cyber and physical security incidents.
- Including cyber-related issues within emergency response plans, and whether and how that relates to the current SEMA initiative to rework emergency response plans within the emergency support function (ESF) frameworks' all hazards approach, specifically ESF12 – Energy

II. Safeguarding Critical Infrastructure Information

A. Is there a need for additional protections other than those already in place to safeguard critical infrastructure security information?

Shielding security information on critical infrastructure from public disclosure is currently subject to widely varying interpretations. Are there structural or procedural protections that could be created or enhanced to prevent security information from public disclosure thereby enhancing information sharing between utilities and the PSC?

B. What would those additional protections look like?

Sections 610.021(18) RSMo and 610.021(19) RSMo provide exceptions to the general rule concerning open public records for state critical infrastructure and security information. Can this language be used as a basis for additional exceptions to open public records? What protection does Section 386.480 RSMo provide? What other protections are in federal law and rules that could be used as a basis for any such proposed language? Are there procedural steps that can be taken in sharing information that would prohibit disclosure?

III. Cyber security standards and monitoring

A. Considering cyber and critical infrastructure presidential directives and orders, how can the PSC assist in partnering with federal agencies in support of these directives and orders?

While both the Presidential Policy Directive "United States Cyber Incident Coordination" (PPD-41; July 26, 2016), and the Presidential Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 11, 2017) are directed primarily at the federal responsibilities and response to cyber security and critical infrastructure, both use language indicating coordination with "State, local, tribal, and territorial governments, and with others as appropriate."

B. How can the PSC assist the harmonization of federal and state oversight responsibilities?

The April 2017 failure at the Larkin Street substation, a substation classified as "Low Impact" by NERC CIP Version 5, caused a considerable system failure in San Francisco. It is reasonable to assume that if asked after the outage, the average San Franciscan would consider the effect of another failure at the Larkin Street substation more than "Low Impact." Are there infrastructure entities in Missouri, not only within electrical utilities, that are 'in the middle'; not classified by either federal or state rules as having a high impact on customers if a failure should occur? How might these entities be identified in all utilities in Missouri? What role, if any, should the PSC have in assisting in the harmonization of state and federal responsibilities that might identify these types of infrastructure assets?

C. Is there a need for cyber and physical security performance measures and metrics?

For Missouri regulated utilities there are currently few reporting requirements for security-related incidents, whether cyber-related or not. Is there a need for new security-related reporting requirements? If reporting were to be required, how might the information reported be used to improve security? What would constitute a reportable incident and how might that be determined? How would reporting relate to and/or improve "safe and reliable utility services at just, reasonable and affordable rates"?

What measures and metrics are currently used in the security realm, both cyber and physical? Would reporting of these measures and metrics improve security and assist other utilities in improving security by identifying best practices? Can these measures and metrics be modified to be utility customer-centric? Would reporting in a manner similar to SAIDI/SAIFI-CAIDI/CAIFI be useful in improving a utility's ability to provide "safe and reliable utility services at just, reasonable and affordable rates"?

D. Risk analysis and risk management

What methodologies are being used when performing risk analyses and risk management? How might these methodologies be improved? Can a mutual aid paradigm assist in risk management at the edges of an individual utility's service area?

E. Cyber and physical security personnel and functional responsibility

Contact lists of security personnel available on a need-to-know basis would help in communications between utilities, regulators and first responders during and after a security event. Is there a need for a functional listing of utility security personnel? Where might such a list reside and what protections are needed to limit public disclosure? What other information might be included? Are any such mechanisms already available and currently being used? If so, to what extent are those being used?

IV. Cyber related information sharing

A. Should the PSC develop a formal group for cyber-related information exchange and/or monitoring between utilities?

The April 2017 Council on Foreign Relations contingency planning memorandum "A Cyberattack on the US Power Grid" states that the Government Accountability Office found "unlike the financial and defense industrial base" "cybersecurity information sharing [was] weak" across the energy sector. How can the PSC support information exchange between utilities? Should a formal information exchange group be developed? If there were a formal exchange mechanism, what would be the content of the information to be shared? What would the limitations be? How would those be determined?

B. Just as in the case of storm recovery, should a formal cyber-related mutual aid and assistance plan be developed?

What might a cyber-related mutual aid plan include? Unlike the storm recovery mutual aid, the systems and processes that would be supported might vary widely. Different software, hardware, processes and procedures might hamper effectiveness. Would an information/training exchange process need to be included in such a plan? How might a utility evaluate the fitness for support of any particular individual from another utility?

C. Should the PSC support monitoring intelligence feeds and pushing out intelligence products for events related to Missouri?

The PSC has developed and is in the process of formalizing a relationship with the Missouri State Highway Patrol (MSHP) by way of the Missouri Information Analysis Center (MIAC). Are the current intelligence feeds sufficient for security at Missouri utilities? Might there be value in a new Missouri-centric critical infrastructure intelligence feed? What do utilities see as a void in the intelligence feeds currently being used? How might the PSC assist in filling such a void?

V. Cyber hazards and the State Emergency Management Agency (SEMA) harmonization of emergency response plans in ESF12

A. Emergency response plans harmonization

SEMA is currently reworking emergency response plans into the ESF framework. The PSC is the lead agency for ESF12, Energy. Should cyber-related risks be contemplated while reworking ESF12 emergency response plans? How might that be accomplished? Would a cyber-related event differ from a storm-related event? What might be the differences? What would the effect of those differences be? How can those differences be addressed? How can issues pertinent to utilities not currently working on the rework of ESF12 be included? Which utilities might that be, if any?

B. Should all Missouri utilities submit updated emergency response plans on a recurring basis?

Should utilities submit response plans to PSC? If not, why not? What might be included in those plans? What should be excluded? How can those plans be shielded from public disclosure? Should those plans be submitted directly to the PSC or through cooperation with another state agency, such as the MSHP?

STATE OF MISSOURI

OFFICE OF THE PUBLIC SERVICE COMMISSION

I have compared the preceding copy with the original on file in this office and I do hereby certify the same to be a true copy therefrom and the whole thereof.

WITNESS my hand and seal of the Public Service Commission, at Jefferson City, Missouri, this 13th day of June 2017.

Morris L. Woodruff
Secretary

MOPSC
Digitally signed by MOPSC
DN: cn=MOPSC
Date: 2017.06.13 16:47:54 -05'00'

MISSOURI PUBLIC SERVICE COMMISSION

June 13, 2017

File/Case No. AW-2015-0206

Missouri Public Service Commission
Staff Counsel Department
200 Madison Street, Suite 800
P.O. Box 360
Jefferson City, MO 65102
staffcounselservice@psc.mo.gov

Office of the Public Counsel
Hampton Williams
200 Madison Street, Suite 650
P.O. Box 2230
Jefferson City, MO 65102
opcservice@ded.mo.gov

Missouri Public Service Commission
Whitney Payne
200 Madison Street, Suite 800
P.O. Box 360
Jefferson City, MO 65102
whitney.payne@psc.mo.gov

Enclosed find a certified copy of an Order or Notice issued in the above-referenced matter(s).

Sincerely,

Morris L Woodruff

Morris L. Woodruff
Secretary

Recipients listed above with a valid e-mail address will receive electronic service. Recipients without a valid e-mail address will receive paper service.