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

RESPONSE OF KANSAS CITY POWER & LIGHT COMPANY AND KCP&L GREATER MISSOURI OPERATIONS COMPANY TO COMMISSION QUESTIONS

Kansas City Power & Light Company ("KCP&L") and KCP&L Greater Missouri Operations Company ("GMO") (collectively, "KCP&L" or "the Company") hereby submit comments to Topics for Written Responses and Discussion at the Missouri Public Service Commission Security Workshop issued on June 6, 2017.

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?***

RESPONSE: Because a potential attacker would find any security-oriented information useful in promulgating an attack, anything but the most generic information would immediately become a vulnerability to a utility's security program. KCP&L believes the best way to provide information to the Commission is through face to face meetings with individual utilities.

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?***

RESPONSE: The Company believes that certain information provided to the Commission by a utility is protected from public disclosure under section 386.480 RSMo and that information

regarding cyber or physical security does fall under the open records exceptions found in 610.021(18) and 610.021 (19) RSMo. These non-disclosure protections do not address the level of cyber and physical security at the Commission to protect utility information. For this reason, the Company believes that the best way to share information with the Commission is through face-to-face meetings with individual utilities.

III. <u>Cyber security standards and monitoring</u>

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."***

RESPONSE: If appropriate, the PSC could help the smaller critical infrastructure providers with understanding when and how they need to react to such directives or orders. KCP&L already has the mechanisms in place to handle these interactions between state and federal agencies.

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?***

RESPONSE: It is important when considering the NERC CIP Standards to understand what risk the requirements are designed to mitigate. In the NERC Standards, the term "Low Impact" is used to categorize the risk to the Bulk Electric System. The design is purposefully built to protect the "highway" or infrastructure to enable electricity to be delivered to the distribution system and ultimately the customer. Those protections must be at a higher level of security control given these elements represent a higher target with greater impacts. This does not suggest that security controls applicable to customers are less important but the tactics and application may be different in size and scale. Those elements represented to support protections of the highway scale grid also support the distribution and customer level elements. The NERC CIP Standards mandate physical and cyber security measures in a manner that considers and balances both the potential impact an

outage at a given facility as well as the electrical load it supports. The Company does not believe that any harmonization of state and federal responsibilities is needed. Any new rule protecting critical infrastructure should be considered with the understanding of the potential impact of an outage, risk mitigation desired and willingness of the customer to incur cost of additional security measures.

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 utilities ability to provide "safe and reliable utility services at just, reasonable and affordable rates"?***

RESPONSE: KCP&L already reports security related incidents under federal reporting requirements and does not believe that the Commission should duplicate these reporting responsibilities. KCP&L believes the best way to provide information to the Commission regarding cyber and physical security related incidents is through face-to-face meetings with individual utilities.

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?***

RESPONSE: The Company conducts periodic cyber and physical security assessments to identify gaps and risks. In the past, the Company has discussed these assessments with the Commission and/or its Staff and can continue to do so in the future.

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?

RESPONSE: Contact information for the Directors of Cyber and Physical Security can be provided.

IV. <u>Cyber related information sharing</u>

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?

RESPONSE: KCP&L participates in numerous venues for information sharing and collaborative learning. There are numerous formal information exchange groups in effect and functioning. For those entities that are not parties to these groups, in participation with Southwest Power Pool, they can participate in the discussions. Some of the meetings that relate to these items and opportunities for information sharing or learning are open to their participation without a membership fee associated. KCP&L encourages and supports those entities participation. Most of these venues are face to face meetings with verbal communication of information. For certain forums and information sharing, an NDA may be required by those entities that wish to participate.

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?

RESPONSE: The Edison Electric Institute has already formed a Cyber Mutual Assistance group (consisting of investor owned utilities, municipalities, cooperatives, and regional transmission organizations) of over 100 members. KCP&L participates in this group.

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?***

RESPONSE: KCP&L currently subscribes to many intelligence feeds both inside and outside the utility space. Timeliness of the intelligence is the most important element. KCP&L does not have a need for additional intelligence feeds at this time.

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

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?***

RESPONSE: The Company does not believe that cyber related risks should be included in ESF 12 as these risks are addressed in the Company's incident response plan.

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?***

RESPONSE: The Company does not believe that its plans should be submitted externally as a strong security practice. The Company has an obligation to protect its assets and systems, thus the sensitivity to release of material that can be used for promulgation of attacks. The transfer of cybersecurity risk to other entities when the information is held in their systems introduces an risk to the Company systems. As indicated earlier, the most effective way for the PSC to exercise oversight and participate with the Company is to provide information to the Commission through face to face meetings with the individual utility(ies).

Respectfully submitted,

/s/ Roger W. Steiner

Robert J. Hack, MBN 36496
Roger W. Steiner, MBN 39586
Kansas City Power & Light Company
1200 Main Street, 19th Floor
Kansas City, MO 64105
Telephone: (816) 556-2791
Telephone: (810) 556-2314
Facsimile: (816) 556-2110
E-Mail: Rob.Hack@kcpl.com
E-Mail: Roger.Steiner@kcpl.com

Attorneys for Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company

CERTIFICATE OF SERVICE

I do hereby certify that a true and correct copy of the foregoing document has been hand delivered, emailed or mailed, postage prepaid, this 5th day of July, 2017, to all counsel of record.

/s/ Roger W. Steiner

Roger W. Steiner

Attorney for Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company