BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION

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

ITC MIDWEST LLC'S RESPONSE TO THE COMMISSION'S NOTICE OF OPPORTUNITY TO COMMENT

COMES NOW, ITC Midwest LLC, and for its response to the Commission's questions identified by staff, states as follows:

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:

ITC believes there is a strong need to enact federal and state legislation to protect information related to critical infrastructure and threat intelligence from public disclosure. Utility infrastructure information provided to, or held by the PSC, should be considered confidential and protected from public disclosure. Disclosure of critical infrastructure information by government and state agencies continues to be a risk for utilities when sharing information with such entities. Exemptions to the Freedom of Information Act (FOIA) and Missouri's Sunshine Law should be enacted to provide protection against disclosure of critical infrastructure information.

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:

Any proposed legislation should include broad protections for information related to cyber security and critical infrastructure information that is developed, received, maintained or held by the PSC. These protections should include language making cyber security information and critical infrastructure information confidential and an exception to open record laws. The law should also broadly define cyber security information and critical infrastructure information.

State of Iowa House File 445 and House File 601, provide good examples of legislation aimed to protect critical infrastructure and security information held by its governmental entities.

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."

Response:

The PSC should primarily focus on communicating cyber security or critical infrastructure intelligence and/or information to potentially affected utilities in a timely manner. The PSC should also encourage participation in federal initiatives and provide any associated rate-based action necessary to allow for such participation.

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:

Utilities' high, medium, and low impact assets are governed by NERC CIP. The PSC should determine where they may be able to work with utilities to contribute information on what could be considered as having a "high impact" on customers through PSC resources, county emergency managers, etc.

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"?

Response:

Reporting requirements under NERC Cyber Security and Reliability Standards have already been established with internal control assessments being performed by utilities which include many measures as part of the standard to gauge performance and controls to protect the applicable assets.

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:

From an emergency management perspective, known risk factors (which are normally determined in each state's hazard risk analysis (THIRA, etc.)) are used as a basis for determining the most probable types of events that may affect a utility. An improvement

to this long term average look at risk can be achieved through a review of current trends resulting from weather patterns, civil issues, and other risk related matters to provide additional risk determination data points.

Mutual assistance can certainly be used to recover from outages more quickly and effectively. However, an issue with mutual aid availability is the source and extent of an outage or incident. The source and extent of an outage or incident is something utilities normally consider in their event reviews, and often leads to expanded requests from mutual assistance groups not located in the immediate area. Requests from outside the immediate area are done to increase the likelihood mutual aid responders are not affected by the same outage or incident. Therefore, the mutual aid paradigm is already considered as part of the risk analysis and risk management process.

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:

ITC is not aware of a published list of contact information for security personnel. A contact list of security personnel could be helpful, but would require information protection controls to ensure privacy and confidentiality.

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?

Response:

The PSC could develop a cyber-related information exchange. ITC recommends that events between the PSC and local utilities be organized and facilitated outside of a PSC

facility. Utilities should be assured the information exchange is kept private to encourage sharing while the PSC acts only as a coordinating entity to provide for an open exchange among peers. A non-disclosure agreement should be established amongst the utilities to protect confidentiality.

Enhanced efforts have been made to facilitate information exchange among public safety entities and private sector partners through the establishment of fusion centers in each state that serve to maximize the ability to detect, prevent, apprehend and respond to criminal and/or terrorist activity. Fusion centers combine expertise from these entities to analyze both classified and unclassified information and provide the resulting intelligence to federal, state, and local groups. This process achieves a higher degree of security for the country, provides federal entities with information that was previously difficult to obtain, and is very beneficial to state, local, and tribal governments, as well. It would be very helpful if the PSC encouraged sharing through the state fusion center rather than directly through the PSC. This would help with information security and promote the participation of other State resources. There are several states that have adopted this format for the exchange of information between utilities and the PSC might find it useful to look to those for examples of how such exchanges might be structured. For example, in Iowa, ITC is a member of the Iowa "Private Sector Resource Coordination Work Group," consisting of electric utilities, the Iowa Division of Intelligence and Fusion Center, the Iowa National Guard, the FBI, Iowa Homeland Security, and several others. The group started having quarterly meetings in January 2017, and is linked through the Homeland Security Information Network (HSIN), and RISSNET (Regional Information Sharing Systems) secure internet sites. Internal communications are subject to mutually agreed-upon security measures to avoid potential disclosure of critical infrastructure information to outside entities.

In Iowa, the Iowa Utilities Board (IUB) is involved with the Fusion Center to assist with the exchange of information in emergency response efforts and exercises. The IUB initially arranged a meeting in which utilities could explain their outage restoration and coordination processes to the IUB and other state agencies. The IUB then followed by hosting state power outage exercise planning meetings, participating in bi-weekly exercise planning calls, and attending a joint utility exercise planning meeting outside of the IUB's home office. IUB personnel also participated as players in the resulting full-day joint utility exercise conducted in September 2016. ITC feels this is a valuable way to coordinate and maintain relationships with the State and State agencies, and ITC encourages the PSC to aid in developing similar efforts in Missouri.

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:

A few industry groups, such as the Edison Electric Institute have established a Cyber Mutual Assistance Program. ITC participates in the EEI program. The program requires significant investment in terms of time, money, travel and personnel and therefore the viability of the program is yet to be determined. Mutual assistance programs can be a great help to small utilities such as municipal utilities and cooperatives.

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:

Fusion centers for aggregating threat intelligence and providing fast reliable information can be a valuable resource. ITC believes a Missouri critical infrastructure intelligence feed would be a great asset, provided it is confidential and protected from public disclosure. A critical infrastructure feed would be an excellent way of providing significant intelligence on a localized basis.

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?

Response:

Yes, cyber-related risks occur every day and should definitely be considered in emergency response plans. While the rapidly changing scope of cyber-attacks cannot be

specifically described, a generic process of observation, noting effects, etc., can be applied.

A cyber-related event may occasionally affect systems in a manner similar to storms. However, they are usually very different in the aspect of physical damages incurred. Therefore, physical and cyber events must each be specifically addressed in the reworking of the 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:

For the following reasons, utilities should not submit emergency response plans to the PSC:

1. Without a guarantee of a FOIA and Sunshine Law exclusion, there is a concern for public disclosure of critical infrastructure information. Furthermore, many documents are designed for utility personnel. Individuals who are not routinely exposed to the information may not understand the criticality of some data.
2. Providing emergency plans to the PSC also introduces the potential for discrepancies or misunderstandings between PSC personnel and utility personnel as the PSC may not have the most up-to-date information. Plans and processes used by utilities are frequently adjusted to incorporate lessons learned, best practices, etc. Requiring utilities to submit response plans to the PSC on a regular basis, or as changes occur to the utility's emergency response plans, also introduces a cost element for utilities.

If the PSC seeks information regarding utilities' emergency responses plans, the responses should be limited to the titles and purposes of the utility's emergency plans. For confidentiality and control, all plan details, processes, personnel information, and critical infrastructure specifics should be excluded. The titles and purposes should be sufficient to establish that utilities have the necessary capabilities to manage adverse events.

Respectfully submitted,

CURTIS, HEINZ,
GARRETT & O'KEEFE, P.C.

/s/ Carl J. Lumley

Carl J. Lumley, #32869
130 S. Bemiston, Suite 200
St. Louis, Missouri 63105
(314) 725-8788
(314) 725-8789 (FAX)
Email: clumley@chgolaw.com

Attorney for ITC Midwest, LLC

CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing have been electronically mailed to Staff and Public Counsel this 5th day of July, 2017.

/s/ Carl J. Lumley