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

LIBERTY UTILITIES' RESPONSE TO COMMISSION NOTICE

COME NOW The Empire District Electric Company, The Empire District Gas Company, Liberty Utilities (Midstates Natural Gas) Corp., and Liberty Utilities (Missouri Water) LLC (collectively, the "Liberty Utilities" or "Liberty"), by and through counsel, and respectfully state as follows to the Missouri Public Service Commission ("Commission"):

1. On February 27, 2015, the Commission opened this docket to address security practices for protecting essential utility infrastructure. On June 6, 2017, the Staff of the Commission ("Staff") submitted an agenda for an upcoming workshop and questions directed to the Missouri utilities, with a request that the utilities respond by July 5, 2017.

2. On June 13, 2017, the Commission issued its Notice inviting responses to the Staff's agenda and questions. As their response, the Liberty Utilities state as follows:

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?

Liberty's Response: Information sharing, though beneficial, often has potential risks. This was evidenced recently by the Burlington Electric event in which information was shared with the DOE that resulted in unauthorized disclosure and a major media event. There are a number of protections that, if implemented appropriately, would provide assurance of proper protection and confidence when sharing sensitive information. DHS PCII and DOE ECII data classifications both have data protection programs and requirements defined as well as penalties for mishandling. Though these programs may

not be applicable for utility to utility information sharing, they could be for utility to Commission or other information aggregating entities such as a Fusion Center.

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?

Liberty's Response: The language does not provide sufficient protection. The current language limits the scope to (18) "any public agency responsible for law enforcement, public safety, first response, or public health." Liberty historically has not been identified as one of these agencies. (19) "Nonpublic entity owning or operating an infrastructure" would include publicly traded utilities, but the clause "for use by that body to devise plans for protection of that infrastructure, the public disclosure of which would threaten public safety" leaves it up to interpretation and may cause concern if the receiving government entity has a difference of opinion of the safety or security impact. Additionally, "Existing or proposed security systems and structural plans" limits the information that would be afforded the protection and may not cover security event information that would help in situational awareness or identifying or responding to security threats.

What protection does Section 386.480 RSMo provide?

Liberty's Response: Section 386.480 states, "No information furnished to the commission by" "public utility" "shall be open to public inspection or made public except on order of the commission". A Commission order to share information could expose the shared information to public disclosure. Also, the violation language may not be strong enough, in the age of "government leaks."

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?

Liberty's Response: An information protection and data handling program would be required to provide the structure details needed to allow utilities to share sensitive information with assurance that the information is protected from breach and unauthorized disclosure. As stated, there are data classifications and programs, like PCII and ECII, that could be a model used by the state to develop the needed program. The

implementation and sustainability of these programs require time and resources to mature to a level of assurance that shared information has proper protection. If all stakeholders were versed, and agreements were made, a data classification procedure would identify the protection and handling requirements for the information, including the limitation of disclosure. Recently, FERC released a final draft, "Best Practices for Controlling Sensitive Material". This guide may be useful for assessing and implementing a program to manage sensitive information.

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 utilize language indicating coordination with "State, local, tribal, and territorial governments, and with others as appropriate."

Liberty's Response: Critical infrastructure consists of 16 sectors, which include communications, dams, energy, and water/wastewater. Some larger utilities may also have nuclear reactors or commercial facilities that are also identified as a critical infrastructure. One challenge in coordination is the designation of sector specific agencies responsible for the appropriate protection of these assets and the approach that each takes. EPA is the agency for water and wastewater; DOE is the agency for electric and gas; with DHS as the responsible agency for dams, communications, commercial facilities and nuclear reactors. DHS TSA also has gas pipeline security responsibility. The PSC could assist by understanding all of the sector specific requirements. They could work with the applicable agency to ensure that a state level plan exists to address and facilitate the containment and recovery in the event an incident impacts multiple sectors. Many of the utilities, including Liberty, have 4 or more critical infrastructure assesses; each of which has a different sector specific government agency that is responsible.

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?

Liberty's Response: The Energy Policy Act of 2005 created the term Bulk Power System (BPS). The NERC glossary of terms identifies the Bulk Electric System (BES). The BES definition is used to determine the scope of the NERC regulatory requirements. We want to clarify that the NERC CIP-002 through CIP-011 standards address the cyber security and the physical protection of cyber assets and CIP-014 is the physical protection of very large transmission substations. The above example highlights the difference in the definition of bulk power system and bulk electric system and the distribution networks. The NERC standards are limited to BES assets that meet specific thresholds, and customers affected is not a measure in assessing impact. They are focused on the reliable operation of generation and transmission assets and load and capacity is the primary measure. The major impact of the above event is a result of a distribution asset. These types of events may support the opinion that the continued changes to compliance requirements will encourage entities to focus on compliance and man not promote or allow resources to focus on a risk based and continual assessment approach to security and the reliable operations of all critical systems.

It would be prudent of the Commission to have a list of critical objectives that they would request that all utilities provide information on how they are addressing the security and reliability of the critical assets that could impact the objective. A risk assessment model could be adopted or developed to identify high impact assets based on the customer or public safety. The expected oversight and level of security controls would depend on the impact of the assets. This would support the risk based approach and would allow the focus to be on major impact assets and would prevent the undue burden and resources to focus on the assets that are not as critical. We should remain cognizant that regulatory requirements prevent the utilization of limited recourse to address security as they may only have time to address compliance.

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 utilized 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"?

Liberty's Response: Well thought out measures and metrics would provide information that could be used by the Commission to determine where attention and resources should be focused. Depending on the level of effort to generate the report, the metrics could be shared on quarterly, bi-annual, annual or periodic bases. We would recommend having a separate definition and process for event or incident reporting.

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"?

Liberty's Response: Security measures and metrics have long been debated and there are endless lists of measures or metrics that could be used. It is recommended that a security strategy be developed and security objectives defined. At that point the measures and metrics to support those objectives could be identified. NIST SP800-55 rev 1 is an information security performance measurement guide and may be a useful resource when determining what will be reported.

D. Risk analysis and risk management - What methodologies are being utilized 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 utilities service area?

Liberty's Response: We currently use a combination of risk assessment methodologies based on industry and functional best practices. The specific methodology is determined by the scope and/or assets being assessed. A common risk definition across all mythologies is used. The Critical Infrastructure RAM-White Paper identifies the following risk estimation.

RISK- Risk is quantified by the following equation:

R = PA * (1-PE) * C

Where: R = risk associated with adversary attack

PA = likelihood of the attack

PE = likelihood that the security system is effective against the attack

(1 – PE) = likelihood that the adversary attack is successful (also the likelihood that security system is not effective against the attack)

C = consequence of the loss from the attack

Though the referenced RAM is focused on a physical risk assessment, the same process could be adapted and followed for cyber risk assessments as well. NIST, COSO, ISO, ISACA, ASIS and other standards organization as well as DHS, DOE, DOD and other government organizations have risk assessment and management guides and methodologies defined. NARUC released a "Risk Management in Critical Infrastructure Protection" documents that describes some basic risk management approaches that could be leveraged. A simplified and basic method that all utilities could easily leverage to assess their critical assets would provide common language and communication among the Missouri utilities. It would allow entities with limited resources to be able to implement the methodology. If a standard risk methodology is created, the possibility to leverage neighboring utilities to assist in the assessment may be plausible.

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 utilized? If so, to what extent are those being utilized?

Liberty's Response: As information sharing and response capability has been enhanced over the past few years, a number of intelligence sharing communities have been created. DHS HISN, FBI InfraGuard and MIAC Fusion Center are examples of critical infrastructure protection resources that utility members could participate in. Some of these resources have the ability to search the members list to identify the security resources of the participating organization and companies. The E-ISAC, DNG-ISAC, Water-ISCA and NCCIC are examples of sector specific organizations that critical infrastructure owners could participate in. Each has contact information for their members. The E-ISAC specifically requested and maintains the emergency contact

information for its owner / operator members. Liberty is a member of all the above organizations.

To ensure the easy and timely communication in the event of an incident, a list of security contacts for MO utilities, reviewed annually, may be appropriate and could be maintained by the Commission. If the submission is voluntary, it would be protected under 610.021(19) RSMo.

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" stats 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 the content of the information to be shared? What would the limitations be? How would those be determined?

Liberty's Response: Information sharing is a very broad topic. As there are a number of agencies already responsible for intelligence and security attack information sharing, we would not recommend the Commission attempt to facilitate that. We recommend the PSC understand all the information and intelligence reporting options for critical infrastructure entities and encourage utilities to participate as appropriate.

The information sharing of security program design and implementation, lessons learned, policy and procedure examples or technology selection may be a great opportunity. This would allow utilities to leverage experience from other utilities. IT would also provide awareness and training for some utilities that may not have mature security programs or in-house security resources. The Missouri Energy Cybersecurity Coalition (MECC) was intended to be this type of program. The Commission could encourage utility participation with MECC and provide topics and resources to be addressed and shared among the members. Be aware that some utilities operate in multiple states and the time and resources needed to attend different security meetings for each state, they operate in, may be a burden.

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?

Liberty's Response: EEI is currently pursuing a cyber mutual aid program, for their members. Storm recovery and mutual aid for physical events are well established and have proven effective. Due to the issues listed above, a cyber mutual aid program would be much different. A cyber mutual aid program would be very difficult to implement and may not be as effective in practice as it is in theory.

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 utilized? How might the PSC assist in filling such a void?

Liberty's Response: The Commission should maintain appropriate situational awareness for the threats and events that could impact Missouri utilities. The MIAC is a great resource for intelligence. For utility specific, the ISACs are also a good source to monitor. The concern with these and all other intelligence feeds are they provide a lot of information but without a security analyst reviewing and understanding the information, the intelligence may not be actionable. A Missouri focused critical infrastructure intelligence feed, provided through the MIAC or other intelligence resource, could be very beneficial. The benefit would only be gained if they not only provided the information about activities and events, but translated that into actionable information that identified security program areas or specific controls that mitigate the threat and/or vulnerability. This information could be used by critical infrastructure asset owner / operators to assess and managed their security programs appropriately. If the information is not actionable, it will be another source for repetitive intelligence information.

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?**

Liberty's Response: It could be very beneficial to update the ESF 12, Energy to identify the roles and responsibilities of the various government agencies, including the resources and services they provide. Cyber related function for each of the existing agencies could be included providing a single source to identify available resources and responsible agencies for both cyber and physical events. One needed update, to include cyber event in the ESF 12, is to add the Department of Justice as a support agency. The FBI was named as the primary response agency for cyber threat response events in Presidential Policy Directive PPD-41.

One difference between a physical or operational event and a cyber event is that most utilities have qualified individual or resources to assess and appropriately respond to physical and operational events that affect utilities. Cyber assets (both IT and OT) do not have the same structure or standards as physical infrastructure or the number of qualified resources to appropriately respond. Cyber security resources are in a much shorter supply and cyber responses vary greatly, depending on the type of security threat and the assets impacted. Another complexity to the issues is, storm events that have great impact on our infrastructure have been occurring for some time and the response and approach has matured over many years. The cyber threats that could cause have a negative impact on critical infrastructure and require a response is still being discovered and is constantly changing. This is not to say that we are vulnerable or planning is not possible. It is more that we have to manage the known risks and leverage a continued assessment and improvement approach, as the threats and vulnerabilities are constantly changing. The ESF update could highlight response plans and key resources and contacts needed for containment and impact assessment resources and to have plans that would assist in recover and restore function that may be needed for critical systems.

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?

Liberty's Response: We do not feel that a yes or no answer is appropriate. As with most security related questions; it depends. Emergency response plans can vary by scope and detail. A high-level response plan for physical events or loss of cyber assets, that could impact critical infrastructure, may be able to be shared with little concern. The information in a detailed plan could be highly sensitive. If the sensitive information is redacted prior to submitting, it may not provide value to the PSC. The discussion on data protection above covers the issues if the response plan is submitted with sensitive information.

The MSHP or DHS PSA may be able to provide an assessment of the emergency response plans of critical infrastructure assets owners and operators. This would prevent the need to share the information in a way that could put it at risk of public disclosure and would help build relationships between the state utilities and state and regional security partners.

Alternatively, Liberty has been and will continue to full cooperate with the PSC for plan review and information sharing through verbal conversations and onsite visits. The meetings are understood to be sensitive and the information is retained by and in the control of Liberty. We may be open to a joint meeting/review with the PCS and MO-OHS, MSHP or DHS PSA for a review of the plans.

3. The Liberty Utilities are committed to helping to ensure the appropriate protection and reliable operation of the services provided to their customers. In order to better understand the Commission's intended direction and to help frame recommendations and possible solutions to improve the security of critical assets, it would be beneficial to know the Commission's approach to the following questions, which are taken directly from the NARUC cybersecurity primer:

a. What scope do you want your strategy to cover? What sectors? How deep do you want to go?
b. How does the Commission want to prepare itself? What staffing and resources will be allocated? What training?
c. Who will be responsible internally? Are new policies needed internally?

d. What performance requirements do you want from the company?
e. What reporting/communication do you want before, during, and after a potential cyber event?
f. Will your interactions with the utilities and other stakeholders be formal or informal?
g. Do you want to actively encourage utilities to make cyber investments? Do you want to describe known issues that could constrain investment?
h. Who else will you work with (law enforcement, information technology, etc.)?
i. What else do you need to learn to be ready?

4. For Staff or Public Counsel inquires of the Liberty Utilities in this docket, Shawn Eck may be contacted by e-mail at seck@empiredistrict.com or by phone at (417) 626-5957.

WHEREFORE, the Liberty Utilities respectfully submit their Response to Commission Notice and request such relief as is just and proper under the circumstances.

Respectfully submitted,

BRYDON, SWEARENGEN & ENGLAND, P.C.

By:

/s/ Diana C. Carter
Diana C. Carter MBE#50527
312 E. Capitol Avenue
P. O. Box 456
Jefferson City, Missouri 65102
Phone: (573) 635-7166
Fax: (573) 635-3847
E-mail: dcarter@brydonlaw.com

CERTIFICATE OF SERVICE

I hereby certify that the above document was filed in EFIS, with notification of the same being sent to all parties of record. I further that a true and correct copy of the above document has been sent by electronic mail on this 5th day of July, 2017, to the Commission Staff (Nathan Williams) and the Office of the Public Counsel (Hampton Williams).

/s/ Diana C. Carter