Topics for Written Responses and Discussion at the Missouri Public Service Commission Security Workshop - July 2017

I. 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?

SUI IT Response: Publishing minimum encryption/file-protections standards for information "at rest" and in transit would be one of the protections to consider between the PSC and 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?

SUI IT Response: No recommendations for the cited sections or any applicable statutes.

II. 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."

SUI IT Response: No recommendations for the cited directives or any applicable statutes though Infragard (FBI facilitated) is an excellent federal resource to utilities.

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?

SUI IT Response: No recommendations but agree with the assessment need for unknown "weak links" or single-points-of-failure within all utility systems.

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"?

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"?

SUI IT Response: Published minimum standards in line with a widely known cybersecurity framework such as NIST (National Institute of Standards and Technology) would be of value for utilities and provide a baseline for assessment. The American Gas Association already requests annual self-assessments (NIST based) for which Summit Utilities, Inc. does participate.

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?

SUI IT Response: Summit Utilities, Inc. manages overall systems risk utilizing a self-assessment approach with annual third party reviews for cybersecurity considerations. Our participation in industry and other groups such as Infragard and DNG-ISAC has included noting the desire on an industry level the need to more easily and securely facilitate mutual aid and information sharing during widely impacting events such as the recent 'wannacry' ransomware outbreak.

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?

SUI IT Response: Summit Utilities, Inc. would provide contact information for cybersecurity coordination purposes. Infragard and DNG-ISAC are existing organizations that SUI participates in that maintain contact lists for this purpose.

III. 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?

SUI IT Response: Summit Utilities, Inc. participates in the Missouri Energy Cybersecurity Coalition which was quite active through 2016 for information exchange. Strengthening relationships with organizations such as it would be of excellent value.

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?

SUI IT Response: Working with the Missouri Energy Cybersecurity Coalition could provide an effective approach to developing protocols for cyber-related mutual aid practices. Just doing an initial table-top exercise would generate a large number of ideas and identify considerations for this potential approach to putting in place response management.

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?

SUI IT Response: A feed possibly for utilities known to not be Missouri Energy Cybersecurity Coalition, Infragard, or DNG-ISAC members could be of value. Currently Summit Utilities, Inc. is comfortable with the scope of information provided by our existing relationships with these organizations as well as our software and hardware providers.

IV. 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?

SUI IT Response: No recommendations for the cited considerations.

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?

SUI IT Response: Summit Utilities, Inc. expects that we would comfortably participate in providing this information through our existing practices and programs but would recommend that the PSC consider asking only for voluntary submittal of audit finding reports verifying the existence of effective utility emergency response plans.