**Missouri-American Water Company’s Comments for Cybersecurity and Physical Infrastructure Security Workshop**

**Safeguarding Critical Infrastructure Information**

*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?

*We see this as an evolving and improving space. The development of robust controls is paramount to protecting information that is deemed sensitive. At the Federal level, programs like the Protected Critical Infrastructure Information (PCII) Act can be used as an example.*

*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?

*The PSC should ensure that existing rules appropriately protect security sensitive information and procedures developed to ensure those rules are effective when sharing information.*

**Cyber security standards and monitoring**

*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.”

*This may be better directed to DHS. However, in the private sector, critical infrastructure entities are encouraged to take advantage of the DHS Protective Security Advisor \*(PSA) program.*

*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?

*No comments.*

*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”?

*Missouri may want to look to New Jersey, as an example of a state with a critical sector cyber reporting requirement, via their NJCCIC. Consistency in reporting across sectors is key with any reporting requirements. As such, we would recommend the PSC establish a cross functional workgroup to develop criteria for reporting.*

*In terms of measures and metrics, using tools like the Cybersecurity Capability Maturity Model (C2M2) is a way of measuring across sectors and providing consistent results. Leveraging the DHS CSET tool or having a C-IST performed would benchmark a company against their own sector.*

*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?

*Within the Water Sector, the American Water Works Association (AWWA) J100 risk and resilience tool is the preferred voluntary standard. The AWWA has also created the Cybersecurity Guidance Tool, which is supports implementation of the NIST Cybersecurity Framework.*

*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?

*We see significant value in, and would support the creation of, a centralized contact list. We would prefer the list include both individual contacts as well as access to any/all 24x7 operations center contacts. We are not aware of any existing location, of a contact list, as it stands today. One thing to note would be that a robust process for maintaining the list would need to be developed.*

**Cyber related information sharing**

*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?

*We do not recommend the PSC develop their own information sharing network, however we would like to see the PSC support usage of the existing information sharing networks such as ISAC’s. In the water sector, we leverage the Water-ISAC, but there also exists the MultiState MS-ISAC, Electricity E-ISAC, and several more. Consistently leveraging the ISACs would ensure sharing within and outside of our respective sectors. It would also leverage an information sharing network that is well defined and matured.*

*The state fusion centers should also be included and are also a great information sharing entity. In Missouri, we maintain a relationship with all three fusion centers (St. Louis, Jefferson City MIAC, and Kansas City TEW).*

*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?

*In the water sector, within the state, there already exists a mutual aid process. The Water and Wastewater Agency Response Network (WARN) is a network of "utilities helping utilities" within a state to respond to and recover from emergencies by sharing resources with one another.*

*For Missouri - <http://moruralwater.org/mo-warn/>*

*What could be expanded, within WARN, would be the availability and sharing of cyber skills and resources and should be coordinated with ISAC’s.*

*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?

*As cyber security and vulnerabilities are generally less state specific and do not have geographic boundaries, data from the PSC/MIAC will be valuable but could also be duplicative to many of the other sources (ICS-Cert, ISACs, other fusion centers, vendor partners, etc.). Integrating with existing information sharing sources vs. developing new sources would be most valuable.*

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

*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?

*Cyber Security should be considered in the ESF planning process to ensure support resources are available to critical infrastructure during a large scale cyber event.*

*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?

*Since individual response plans will vary by utility, and understanding of response protocols, within the response and recovery plan, would be difficult to understand without underlying knowledge of the business and their processes, an alternative approach to submission is attesting to certain key requirements of a plan (i.e. contains cyber security response).*