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**

MISSOURI DIVISION OF ENERGY'S COMMENTS IN RESPONSE TO *NOTICE OF OPPORTUNITY TO COMMENT*

The Missouri Department of Economic Development ("DED") – Division of Energy ("DE")[1] submits these comments to the Staff of the Missouri Public Service Commission ("Staff" and "Commission," respectively) in response to the Commission's June 13, 2017 *Notice of Opportunity to Comment* ("Notice") in the above-captioned proceeding. DE appreciates the Commission's and Staff's continuation of the much-needed dialogue on utility physical and cyber security. Recent events have re-emphasized the need to protect Missouri's critical infrastructure; such events include the cyber attack on Ukrainian power systems and the recent "Nuclear 17" incident.[2]

Several recommendations in the Missouri Comprehensive State Energy Plan ("CSEP") speak to the need for emergency planning. These include recommendations 3.8 (Developing Emergency Planning Partnerships), 3.9 (Establishing a Vulnerability Assessment Working Group), and 3.10 (Planning for Cybersecurity). Specifically, these recommendations suggest: establishing a working group to enhance private energy supplier participation in the overall energy emergency planning process at the local, state, regional, and national levels; establishing

[1] The Division of Energy was transferred from the Department of Natural Resources to the Department of Economic Development on August 29, 2013 by Executive Order 13-03. The Order transfers "[A]ll authority, powers, duties, functions, records, personnel, property, contracts, budgets, matters pending, and other pertinent vestiges of the Division of Energy from the Missouri Department of Natural Resources to the Missouri Department of Economic Development …."

[2] For more on cyber security and Ukraine, see Greenberg, Andy, "Lights Out," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/, pp. 53-63.

a vulnerability assessment working group to prioritize emergency response efforts; continuing collaboration and coordination on cyber security; and, performing a statewide risk assessment of public and private energy-related systems and facilities.[3] The CSEP also includes extensive discussions of the need to address both physical and cyber security.[4]

The Board of Directors of the National Association of State Energy Officials ("NASEO")[5] adopted a resolution on April 27, 2017 that urges states to review and, if necessary, update their Energy Emergency Assurance Coordinators points of contact and ensure that these points of contacts understand their roles and responsibilities under the *Agreement for Enhanced Federal and State Energy Emergency Coordination, Communications, and Information Sharing*. This agreement was renewed last year between NASEO, the National Association of Regulatory Utility Commissioners, the National Governors Association ("NGA"), the National Emergency Management Association, and the U.S. Department of Energy ("USDOE"). The resolution also states:

> … the NASEO Board of Directors encourages state energy officials, regulators, and other agencies responsible for energy emergency planning to review and update state plans as needed to ensure that an *"all hazards"* approach, including energy-related critical infrastructure interdependencies and cyber security, are addressed in the plans. This update should reflect evolving state and federal organizational structures, roles and responsibilities, and other critical planning needs such as responding to petroleum shortages and energy disruptions from

[3] Missouri Department of Economic Development – Division of Energy. 2015. *Missouri Comprehensive State Energy Plan*. https://energy.mo.gov/energy/docs/MCSEP.pdf. Pages 233-234.
[4] See, for instance, Chapter 3, Section III (starting at page 113) and Chapter 4 (starting at page 126).
[5] NASEO is an organization composed of – and representing – 56 State and Territory Energy Offices, including DE.

> cyber incidents. NASEO will continue to support states' efforts to update their energy assurance plans and maintain their preparedness capabilities ….[6]

NASEO has also developed guidance documents to assist states with these updates.[7] The NGA also has resources on security and emergency planning. These include the "Meet the Threat: States Confront the Cyber Challenge" initiative[8] and the Resource Center for State Cybersecurity.[9] The USDOE's Office of Electricity Delivery & Energy Reliability has pertinent information as well.[10]

Additionally, DE shares the concerns expressed by utilities and stakeholders with regard to the need for protecting confidential and proprietary material when sharing sensitive emergency planning information. In light of this understandable caution, DE recommends that the Commission set a course of additional workshops for follow-up discussions that facilitate the productive sharing of sensitive information with appropriate state and federal agency personnel involved in emergency planning. DE recommends including additional stakeholders in the Commission's proceedings on physical and cyber security, such as the Missouri Office of Cyber Security, the National Guard, USDOE, and the U.S. Department of Homeland Security.

The Commission specifically requested input on Section 386.480, RSMo. as it relates to the protection of sensitive security-related information. Under Section 610.021(18), RSMo., the Commission is an agency responsible for public safety; however, this is a narrow exception, so

---

[6] NASEO, 2017, "National Association of State Energy Officials Board of Directors Resolution on Energy Emergency and Cyber Security Planning, Preparedness, and Response," https://www.naseo.org/Data/Sites/1/naseo-resolution-on-energy-emergency-planning-(final-42717).pdf.

[7] See NASEO, 2017, "Guidance on Updating State Energy Emergency Plans," http://www.naseo.org/data/sites/1/documents/publications/(Final)%20Guidance%20on%20Updating%20State%20Energy%20Emergency%20Plans.pdf, as well as NASEO, 2017, "Guidance on Reviewing and Updating Energy Emergency Assurance Coordinators Contacts," https://www.naseo.org/Data/Sites/1/(clean)-guidance-for-the-review-and-updating-energy-emergency-assurance-....pdf.

[8] National Governors Association. 2017. "Meet the Threat: States Confront the Cyber Challenge." https://ci.nga.org/cms/MeetTheThreat.

[9] National Governors Association. 2017. "Resource Center for State Cybersecurity." https://www.nga.org/cms/center/issues/hsps/state-cybersecurity.

[10] See, for example, Office of Electricity Delivery & Energy Reliability, Undated, "Cybersecurity for Critical Infrastructure," U.S. Department of Energy, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure.

closed documents under that section would be limited to guidelines or plans for responding to certain incidents, not those submitted as public documents during the course of an ordinary rate case. Per Section 610.021(19), RSMo., confidential documents related to security systems and structural plans that are submitted to the Commission in order for it to, "devise plans for protection of that infrastructure" should be closed. Section 610.021(14), RSMo. classifies these documents as closed by designating them "records which are protected from disclosure by law," so Section 386.480, RSMo. would apply.

DE thanks the Commission and its Staff for the opportunity to comment.