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

JOINT RESPONSE TO STAFF'S FOLLOW-UP REPORT

COMES NOW Union Electric Company d/b/a Ameren Missouri ("Ameren Missouri" or "Company"), together with Evergy Metro, Inc. d/b/a Evergy Missouri Metro and Evergy Missouri West, Inc. d/b/a Evergy Missouri West (collectively, "Evergy" or "Evergy Companies")[1] and for their *Joint Response to Staff's Follow-Up Report* ("*Joint Response*"), state as follows:

BACKGROUND

1. On March 4, 2015, the Missouri Public Service Commission ("Commission") opened this working docket to address concerns about effective cybersecurity practices for protecting essential electric utility infrastructure. Over time, the Commission expanded this working docket to include all utilities and all physical security threats.

2. On March 23, 2015, Staff held a workshop regarding these issues and subsequently solicited responses from the utilities addressing their cybersecurity practices and emergency preparedness. Staff summarized the information it gathered in a *Report* submitted to the Commission on May 26, 2016.

[1] Ameren Missouri and the Evergy Companies are referred to herein collective as "the companies" or "the utilities." This phrasing is not meant to imply that any non-signatory utility or company engaged in this proceeding agrees with the content of this *Joint Response*.

3. On July 11, 2017, Staff held another workshop, which was preceded by more comments from interested stakeholders. On October 1, 2019, the Commission Staff ("Staff") submitted a pleading entitled "*Staff Follow-Up Report*" ("*Follow-Up Report*"), which contained a discussion of additional data gathered by Staff and several resulting recommendations. Staff requested interested stakeholders to submit responses to its *Follow-Up Report* within 30 days of its submission. On October 2, 2019, the Commission issued an order requesting responses to Staff's *Follow-Up Report* by November 1, 2019.

4. Staff made a total of 21 recommendations based upon the information it has gathered through this workshop docket, sorted into the following seven categories:

- Reporting
- Emergency Communications
- Information Sharing
- Organization Development
- Mapping
- Preparedness and Exercises
- Resource Availability

5. Ameren Missouri and Evergy appreciate the opportunity to respond to the *Follow-Up Report* and provides their comments regarding the recommendations below. As a general statement in response to the recommendations below, Ameren Missouri and the Evergy Companies are both jurisdictional entities subject to Federal Energy Regulatory Commission ("FERC") and North American Electric Reliability Corporation ("NERC") oversight and enforcement. The companies are subject to federal law, which is inclusive of FERC regulations and NERC Standards, that guide the protection and use of Critical

Infrastructure Information ("CII") and Critical Energy Infrastructure Information ("CEII"), collectively “Sensitive Information.”

6. The NERC Standards are narrowly written regarding access to such information; for example, access can only be given to individuals that have a compelling need to have access. Failure to meet this, and other general requirements, subject the companies to violations and penalties. This illustrates an important principle: the companies are held to a high standard, and clear duty, to protect Sensitive Information from disclosure and the companies carry the ultimately responsibility for the Sensitive Information.

7. While the companies have ultimate responsibility for Sensitive Information, they have little recourse or remedy should a third-party inadvertently or purposely disclose the Sensitive Information. The third-parties identified in the recommendations are not subject to the same standards as the companies, yet the companies would continue to be subject to violating the NERC Standards and assessed penalties. Basically, the more systems on which that Sensitive Information resides, the more channels are available for adversaries to attempt a breach of the security. Furthermore, because the companies have a duty to protect Sensitive Information from disclosure (and as a matter of good security practice), the companies cannot rely on or delegate risk to third-party systems to protect Sensitive Information.

8. The principles outlined above highlight some of the security concerns and liability the companies would carry in sharing the Sensitive Information. Those concerns and issues guide the companies’ responses to the suggested collaborative and information sharing recommendations below.

REPORTING

1) Require each Missouri utility to identify, provide, and actively update contact information for both cyber and physical security points of contact. Points of contact should be personnel actively engaged with both cyber and physical security issues and not a member of the utilities' counsel or involved with regulatory liaison activities.

9. The companies are unsure of what value would be added through implementation of this specific requirement. If the intent is to speed notification and access to information during an event, this requirement is unlikely to advance that goal. During an actual cyber or physical infrastructure event, legal and/or regulatory would be providing informal notice to the Commission's staff. The personnel anticipated by this requirement would be and should be otherwise engaged in incident mitigation and/or investigation. The companies are amenable to providing the emails of relevant personnel so that questions can be addressed when circumstances allow, and can establish a review cycle to make sure those email addresses remain updated on an annual basis or other appropriate timeline. Without further information, we suggest this be a reasonable alternative.

2) Require formal disclosure of plans specifically related to emergency response.

10. For the purposes of its recommendations, Staff has defined "formal" disclosure as disclosure made in writing and submitted to Staff for review; "informal" disclosure is accomplished verbally. Neither form of disclosure requires a public filing or disclosure through the Commission's electronic filing system, EFIS. However, as a government agency, the Commission is subject to Missouri sunshine laws. While the current laws appear to protect critical infrastructure information (see, e.g., Section 610.021 RSMo), these laws are still subject to challenge in a court in a manner that would not necessarily be possible if these plans remained in the utility's possession. The companies

can provide access to such plans or redacted copies of such plans. There are risks to both the companies and the Commission for release of such information either electronic or hard copy form. This is a substantive concern as the FERC and NERC strictly govern the storage of critical infrastructure information. Coincidentally, both regulatory bodies have currently proposed new procedures for protection of this type of information, which would minimize information collection and eliminate storage for extended periods while prohibiting publication. NERC's Rules of Procedure[2] Section 1500, Critical Infrastructure, Cyber Security Incident Information ("CSII") and CEII as designated by FERC and the Department of Energy ("DOE") are all information types that must be protected by the utilities. We are both responsible for the safekeeping and accountable for the disclosure of any such information. The industry, with increasing expectations from numerous departments of the U.S. Cabinet, are recognizing substantive expenses to protect the information requested. It is the company's responsibility to prove to the federal regulators that we can ensure the security protocols employed by all third parties, inclusive of regulatory bodies themselves. In addition, by housing this information within the Commission's building or servers, the Commission and/or its staff also become accountable for any disclosures and could lose access to the information on a temporary or permanent basis as a result. (NERC Rules of Procedure Section 1507.)

11. At a minimum, the companies would need to redact any data that could help an attacker exploit the companies' environments. The utilities would need to conduct a security assessment of the environment before providing any data per this

[2] https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20190125.pdf

requirement, and would need subsequent annual reviews for as long as the entity has possession of the companies' data.

12. Ultimately, the companies caution Staff whether it wants to subject itself to this accountability and security risk. We would instead request the Commission consider access to the information on-site at the utility or in a redacted format.

3) Require periodic Commission briefings on current security posture and related activities.

13. The companies are happy to provide periodic Commission briefings on their respective security postures and related activities, as they have done in the past. Each utility would, of course, tailor its briefings appropriately depending on the forum (e.g., at their respective offices or the Commission's offices, in an open meeting or during private discussions as allowed by the Sunshine Laws, etc.). Additionally, since the utilities have ultimate responsibility and accountability for the information, they would conduct discussions related to these matters as appropriate under the circumstances.

4) Require timely informal disclosure of both cyber and physical security incidents and any related response(s) and effect(s).

14. The companies are amenable to providing a timely informal disclosure of cyber and physical security events.

5) Specifically address supply chain risk management during periodic Commission briefings.

15. The utilities have supply chain risk management practices and are also appropriately preparing for the supply chain risk regulatory requirements that become enforceable on July 1, 2020. These requirements were approved by FERC through NERC's Reliability Standards (CIP-013-1) and represent substantial improvements to security practices through supply chain management, however, these requirements also represent

substantive resource commitments. The companies believe that CIP-013-1 strikes a reasonable and practicable balance between adequate infrastructure protections, business needs, and appropriate contract negotiations. The companies suggest that no additional restrictions or legislation of these activities is warranted at this time. The companies are happy to provide periodic briefings on their respective supply chain risk management activities, as appropriate.

6) Investigate CI information storage within the Department of Public Safety (DPS), State Emergency Management Agency (SEMA), or the Missouri Information Analysis Center (MIAC).

16. The companies are amenable to investigating the information storage capabilities of DPS, SEMA, and MIAC. However, given the responsibilities and accountabilities under NERC's Rules of Procedure as described above, the companies caution that such storage may not be advisable, desirable, or even possible regardless of the systems' security protocols, the agencies' and companies' risk tolerances.

7) Monitor governmental and industry efforts to develop cyber security reporting metrics. Implement a reporting mechanism for such metrics should the development efforts produce useful results.

17. The companies maintain that other regulatory bodies are already appropriately monitoring this information and is reporting those metrics on a regular basis. For example, NERC conducts extensive oversight of electric utility infrastructure security and publishes reports, on the metrics associated with its oversight. Please see https://www.nerc.com/AboutNERC/StrategicDocuments/2019%20Proposed%20Industry%20BPS%20Dashboard%20Metrics_Final_v2.pdf for NERC's most recent reporting included in its "2019 ERO Enterprise Dashboard Metrics." Additionally, the Companies comply with the following additional reporting obligations for cyber and physical security events:

- SEC reporting and disclosure requirements;
- DOE reporting and disclosure requirements; and
- Electricity Subsector Coordinating Council and Electric Sector – Information Sharing and Analysis Center reporting and disclosure.

EMERGENCY COMMUNICATIONS

8) Transition cellular communication accounts to FirstNet for those areas that participate in emergency response and/or other emergency and safety related activities.

18. The companies read this recommendation as though it is directed at Staff or state personnel acting as first responders, and do not have concerns with the recommendation if that is the case. If this is meant to be a utility requirement, the companies require additional clarification and information on this recommendation because it could have significant impacts on the companies' current communications models and purposefully redundant communications systems.

9) Commissioners and select Staff members individually investigate transitioning personal phones used for communications during security related activities to FirstNet if prioritized emergency communications are warranted.

19. The companies have no objection to Staff taking the steps it deems appropriate in this regard.

INFORMATION SHARING

10) Encourage utilities to actively participate in the Intelligence Liaison Officer (ILO) program to receive pertinent threat information and provide information on suspicious activities that they may encounter in conducting everyday operations.

20. The companies are happy to participate in the ILO, and in fact, has participated for several years.

11) Proactively inform Missouri utilities about the Sensitive Compartmented Information Facility (SCIF) capabilities at the MIAC and timing of any classified briefings that are taking place for cleared personnel.

21. The companies have no objection to Staff taking the steps it deems appropriate in this regard.

12) Actively participate in the organization and development of a Utility Information Exchange Group and encourage all Missouri utilities to participate.

22. The companies already participate in an active exchange of information between Missouri utilities is happy to continue these activities. The companies do not believe a new group need be formed to accomplish this goal.

13) Actively participate in the improvement of information sharing between the public and private sectors by encouraging the involvement of investor-owned utilities, cooperative utilities, and municipal utilities where possible.

23. The companies already participate in an active exchange of information between Missouri utilities, including all sectors of utilities, and are happy to continue these activities. The companies do not believe a new group need be formed to accomplish this goal.

ORGANIZATION DEVELOPMENT

14) Partner with SEMA and develop a proposal to expand the types of volunteers involved with the Missouri Structural Assessment and Visual Evaluation (SAVE) Coalition as well as the types of evaluations that could be carried out by such members with a focus on structures associated with critical infrastructure and volunteers with knowledge of such structures.

24. The companies express the need for caution regarding this recommendation. A civilian network would need to be highly trained in many circumstances to safely provide appropriate assistance. For example, an untrained person would be inappropriate to assist

with certain issues that could arise at a nuclear facility. These volunteers would also need to be trained on the protection of critical infrastructure information, and would not be able to store certain systems, maps, or drawings either in their homes or on their home computers. This partnership may not be able to produce the results desired without significant training and safety efforts.

15) Investigate the activities and partnerships necessary to create a Civilian Cyber Corps volunteer organization possibly in connection with the SAVE Coalition.

25. As with the previous response, the companies express a significant need for caution about this recommendation. A civilian network would need to be highly trained in most circumstances to provide appropriate assistance with a cyber incident. These volunteers would also need to be trained on the protection of critical infrastructure and proprietary information, and would not be able to store certain systems, maps, or drawings either in their homes or on their home computers. This partnership may not be able to produce the results desired without significant training and safety efforts.

26. Even with training, however, there are other issues with this collaboration. Soliciting volunteers as cyber forensics experts would expose both utilities and those volunteers to liability if they are working cyber events. In an ongoing cyber event or post-breach response context, best practice is to use a specialized cyber forensics and breach firm ensuring the appropriate level of service, expertise, and risk mitigation. These are highly sensitive events with numerous implications to provide assurances to customers and shareholders managing financial and reputational risk.

MAPPING

16) While Staff has no specific recommendations on adoption at this time, the use of Geographic Information System (GIS) technology

does allow for ease of maintenance and production of maps and mapping services such as the identification and publication of certificates areas granted through the Certificate of Convenience and Necessity (CCN) process.

27. The companies already have several GIS endeavors underway. While the identification and publication of certificated areas would indeed be helpful, the companies suggests we should stop short of the disclosure of all the assets within those territories. There could still be concerns regarding critical infrastructure that should be taken into consideration and maps may well require redaction before any publication to mitigate those concerns. The ability to share and ensure the secure storage of this mapping is dependent upon the depth and detail desired. Depending on the depth and detail, different security measures, including limits on how and what could be shared, will need to be implemented.

17) Periodical review, by the Commission, of software options concerning GIS mapping technology.

28. The companies have no objection to Staff taking the steps it deems appropriate in this regard.

PREPAREDNESS AND EXERCISES

18) Continue to actively participate in upcoming statewide emergency response exercises and when possible, participate in other local, regional, national drills and exercises.

29. The companies have no objection to Staff taking the steps it deems appropriate in this regard. The companies note that they have already welcomed Staff participation in past exercise activities, such as NERC sponsored GridEx.

19) Train at least three Staff members on the emergency response Incident Command System Operations to the minimum level of ICS-400.

30. The companies have no objection to Staff taking the steps it deems appropriate in this regard.

20) Periodically update Commission General Procedures GP-7 and GP-7.5, as necessary.

31. The companies have no objection to Staff taking the steps it deems appropriate in this regard.

RESOURCE AVAILABILITY

21) Encourage all utility owners and operators to engage the Department of Homeland Security (DHS) and Missouri National Guard Cyber Team and leverage their respective resources.

32. The companies already engage with numerous local, regional, and federal agencies[3] on security and crisis management measures, regarding physical and cyber security, so it has no objection to this recommendation. We request the engagement should not be *limited* solely to the referenced agencies.

[3] These agencies include DHS, FBI/DOJ, Unite, NERC, E-ISAC, EEI, NRC, EPRI, AGA, etc.

Respectfully submitted,

Union Electric Company
d/b/a Ameren Missouri

/s/ Paula N. Johnson

Paula N. Johnson, # 68963
Senior Corporate Counsel
Ameren Missouri
1901 Chouteau Avenue
P.O. Box 66149, MC 1310
St. Louis, MO 63103
(314) 554-3533 (phone)
AmerenMOService@ameren.com

Evergy Metro, Inc. d/b/a Evergy Missouri Metro and
Evergy Missouri West, Inc. d/b/a Evergy Missouri West

/s/ Roger W. Steiner

Robert J. Hack, MBN 36496
Lead Regulatory Counsel
Phone: (816) 556-2791
E-mail: rob.hack@evergy.com
Roger W. Steiner, MBN 39586
Corporate Counsel
Phone: (816) 556-2314
E-mail: roger.steiner@evergy.com
Evergy, Inc.
1200 Main – 16th Floor
Kansas City, Missouri 64105
Fax: (816) 556-2787

CERTIFICATE OF SERVICE

The undersigned certifies that a true and correct copy of the foregoing document was sent by electronic transmission, facsimile or email to counsel for parties in this case on this 1st day of November, 2019.

/s/ *Paula N. Johnson*