BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of a Working Case to Address)
Security Practices for Protecting Essential) File No. AW-2015-0206
Utility Infrastructure.)

COMMENTS OF UNION ELECTRIC COMPANY d/b/a AMEREN MISSOURI

COMES NOW Union Electric Company d/b/a Ameren Missouri ("Ameren Missouri" or "Company"), and for its Comments in response to the list of topics and questions issued by the Missouri Public Service Commission ("Commission" or "PSC"), states as follows:

BACKGROUND

1. On May 30, 2017, at the Commission Staff's ("Staff") request, the Commission issued its Invitation to Workshop Meeting to various stakeholders to allow an opportunity to discuss issues related to cybersecurity and physical infrastructure security as they affect all Missouri utilities. On June 13, 2017, the Commission issued a list of topics and questions identified by Staff, and asked for stakeholder responses by July 5, 2017.

2. The list of topics and questions includes twelve (12) areas of discussion categorized into four (4) general subject matter areas:

Safeguarding Critical Infrastructure Information

A. Is there a need for additional protections other than those already in place to safeguard critical infrastructure security information?

B. What would those additional protections look like?

Cybersecurity 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?

B. How can the PSC assist the harmonization of federal and state oversight responsibilities?
C. Is there a need for cyber and physical security performance measures and metrics?
D. Risk analysis and risk management
E. Cyber and physical security personnel and functional responsibility

Cyber-Related Information Sharing

A. Should the PSC develop a formal group for cyber-related information exchange and/or monitoring between utilities?
B. Just as in the case of storm recovery, should a formal cyber-related mutual aid and assistance plan be developed?
C. Should the PSC support monitoring intelligence feeds and pushing out intelligence products for events related to Missouri?

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

A. Emergency response plans harmonization
B. Should all Missouri utilities submit updated emergency response plans on a recurring basis?

3. Ameren Missouri appreciates the opportunity to contribute in this workshop and provides its responses in the following paragraphs.

SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION

A. Is there a need for additional protections other than those already in place to safeguard critical infrastructure security information?

4. Information sharing is a key element to a successful and viable cybersecurity program. So yes, continuing to look for even better ways to create an environment where information can be shared quickly and securely is certainly beneficial. Much progress has been made at the federal and industry level, and work continues. Better information sharing at the state and regional levels will improve the cybersecurity posture of Missouri's utilities.

5. Accordingly, certain information protection enhancements may prove necessary when it comes to sharing information with the Commission in certain contexts. Ameren Missouri is subject to rigorous cybersecurity regulation at the federal level by the

North American Electric Reliability Corporation ("NERC"), which has been authorized by the Federal Energy Regulatory Commission ("FERC") to, among other things, ensure the reliability and security of the bulk electric system. Part of this regulation involves the strict and vigorous protection of critical energy/electric infrastructure information ("CEII"). As described by FERC,[1] CEII includes both physical and virtual assets that:

- Relate details about the production, generation, transmission, or distribution of energy;
- Could be useful to a person planning an attack on critical infrastructure;
- Is exempt from mandatory disclosure under the Freedom of Information Act; and
- Give strategic information beyond the location of the critical infrastructure.

Additionally, revealing CEII could negatively impact national security, economic security, public health or safety, or any combination of those three.

B. What would those additional protections look like?

6. It is uncertain what those additional protections would look like. But, it needs to be an environment that is extremely secure and allows broad participation. Active information sharing and exchange are the objectives of all programs of this nature. However, there are two primary challenges:

- Because of security concerns, oftentimes information and intelligence are not actionable.
- Because cybersecurity events occur and evolve with extreme rapidity, information becomes stale quickly.

For these reasons, while it is viable and appropriate for the industry to share this kind of information with its regulators on request, this sharing does not necessarily lend itself to typical regulatory reporting and oversight.[2]

[1] https://www.ferc.gov/legal/ceii-foia/ceii.asp

[2] Ameren Missouri's Crises Management Communications Plans do, however, include communications with the Commission so that it remains apprised of such situations.

7. It is also worth noting, when sharing this information with regulators (such as during NERC audits), special precautions must be taken to ensure this information remains protected to the degree its importance warrants. It is not unusual for utilities to facilitate sharing CEII with their own regulators during NERC Standards audits using specially encrypted ftp sites, password protected and encrypted hard drives, and other highly secure means. Often when paper copies are made, they are stored (at a minimum) in locked file cabinets and should never be left unattended. With this in mind, additional steps would be required by the Commission to ensure the increased protection of CEII.

8. As far as additional statutory protections, existing laws and statutes – including the provision in 386.480(14) RSMo, which arguably allows federal CEII protections to remain closed – appear to be sufficient.

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?*

9. As it stands today, the amount of scrutiny cyber security is given at the federal level through regulators like NERC and FERC, and through industry/regulator coordination groups such as the Electricity Subsector Coordinating Council is sufficient. The Commission’s participation in organizations like the National Association of Regulatory Utility Commissioners (“NARUC”) can foster a good understanding of the balance of state policy with existing industry regulations. However, adding active state-level regulation to the industry’s already well-scrutinized cyber security programs would likely be duplicative, and in a worst-case scenario (e.g., if they accidentally create a conflict with existing regulations) could prove counterproductive.

B. How can the PSC assist the harmonization of federal and state oversight responsibilities?

10. Given the level of regulation of its cybersecurity practices in light of its size and potential system impacts, Ameren Missouri is sufficiently harmonized. However, smaller utilities such as cooperatives and municipals may require additional assistance in this regard.

C. Is there a need for cyber and physical security performance measures and metrics?

11. Of course, metrics are key to a strong cybersecurity program. Control effectiveness, risk mitigation over time, changes in attack activity, and various types of cybersecurity threats are just a few of the metrics Ameren Missouri routinely measures. Cybersecurity programs are tailored to the risks that exist within a utility and the mitigation programs underway. Because of the unique characteristics of each utility, a "one-size-fits-all" metrics program is not practical.

12. That said, there is value in having a consistent set of baseline measures and metrics from which to tailor measures and metrics for a specific utility. Ameren Missouri is working with the Electric Power Research Institute ("EPRI") to develop a baseline set of cybersecurity metrics that utilities could utilize effectively. The Company regularly shares a subset of cybersecurity metrics with Ameren Corporation's executive leadership team, as well as the Audit and Risk Committee of the Board of Directors.

13. Additionally, each utilities' performance measures and metrics are already highly scrutinized by NERC and its regional reliability organizations (in Ameren Missouri's case, SERC Reliability Corporation). This scrutiny includes triennial audits

and the investigation of self-reported incidents. Additionally, a series of CIPv5[3] audits are currently being conducted in addition to NERC's regular CIP audits. An additional layer of regulatory oversight in this regard is not necessary.

D. Risk analysis and risk management

14. For many years, Ameren Missouri has included risk analysis and risk management as key elements of its cybersecurity program. The Company's current program is based on the National Institute of Standards and Technology ("NIST") Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." The Company uses the "all hazards" vulnerability assessment methodology for all security installations. The Company conducts periodic assessments in order to manage its risks, and then conducts periodic assessments and additional assessments as warranted. For example, some assessments are conducted annually, triennially, randomly, or as dictated by crime trends, scheduled events, or as information and intelligence dictate.

E. Cyber and physical security personnel and functional responsibility

15. The Electricity Subsector Coordinating Council's ("ESCC") Cyber Mutual Assistance ("CMA") program (which is discussed more below) is designed to address this very subject. The American Gas Association ("AGA") currently has a similar program, but on a more informal basis. The ESCC's CMA program, however, is in the process of being expanded to include natural gas utilities as well. Several utilities, such as Ameren Missouri, also have assistance relationships in place to aid in dealing with cybersecurity issues.

[3] NERC's Critical Infrastructure Protection standards, version 5.

16. While these types of mutual assistance programs are welcome, the key to supportive cybersecurity relationships remains secure and safe information sharing. Cybersecurity resources are in very high demand, and cybersecurity attacks are subject to no regional or state boundaries and can escalate rapidly. This reality presents a meaningful challenge to developing a CMA program that can rival what is routinely exhibited with storm response in our industry.

17. Ameren Missouri is happy to provide contact information for key personnel with functional responsibility for physical and cyber security for more information.

CYBER-RELATED INFORMATION SHARING

A. Should the PSC develop a formal group for cyber-related information exchange and/or monitoring between utilities?

18. Many utilities are already members of numerous other groups with the same purpose. Ameren Missouri participates in organizations such as, but not limited to:

- Homeland Security Information Network ("HSIN")
- Infragard
- NERC CIP Committee ("CIPC")
- SERC CIPC
- Cyber Security Risk Information Sharing Program ("CRISP")
- AGA Security Committee
- EPRI
- ESCC
- NERC
- United States Nuclear Regulatory Commission ("NRC")
- Edison Electric Institute ("EEI") Security Committee
- Illinois Energy Cybersecurity Consortium ("IECC")
- Missouri Energy Cybersecurity Consortium ("MECC")
- North American Transmission Forum ("NATF") Security Practices Group
- Department of Justice – Federal Bureau of Investigation ("DOJ" and "FBI")
- Department of Homeland Security ("DHS")
- UNITE Security Directors
- UNITE Tiger Team

- Department of Energy (“DOE”)
- Nuclear Industry Institute (“NRI”)
- Nuclear Information Technology Strategic Leadership (“NITSL”)
- Downstream Natural Gas Information Sharing & Analysis Center (“DNG-ISAG”)
- Electricity Information Sharing and Analysis Center (“E-ISAC”)
- Cyber Resilient Energy Delivery Consortium (“CREDC”)
- Energy Impact Partners
- GridX
- Defense Advanced Research Projects Agency (“DARPA”)

19. The Company acknowledges that there is an opportunity for better information sharing across critical infrastructure sectors, and between utilities and their state regulators. We recommend that these opportunities continue to be pursued at the federal level since cybersecurity threats have no geographic boundaries.[4]

B. Just as in the case of storm recovery, should a formal cyber-related mutual aid and assistance plan be developed?

20. Ameren Missouri already has such a plan facilitated through the ESCC. The ESCC is an industry-government partnership which evolved over time from an ad hoc group of industry CEOs, the Department of Energy, and the Department of Homeland Security. The ESCC’s CMA program is “a series of industry initiatives developed … to provide emergency cyber assistance within the electric power industry,” and includes “a Pool of industry cyber experts who can provide voluntary assistance to other organizations in the event of a disruption to the energy grid due to a cyber emergency.”[5] See the attached document titled, “The ESCC’s Cyber Mutual Assistance Program” for additional information. As noted above, the ESCC’s CMA program is in the process of being expanded to include natural gas utilities, which currently utilize a

[4] Should this information exchange also take place at the state level, the Company notes that it must be safe, secure, and have broad adoption in order to realize the desired benefit. Further, such an information exchange would provide additional benefits if it included bordering states because, as already noted, threats to cybersecurity are not subject to geographic boundaries.

[5] See the attachment to these comments at page 2.

more informal process through the AGA. With such plans already in place, additional plans are not necessary.

21. Based on their access to resources such as those the Company notes above, investor-owned utilities may be able to offer assistance to smaller cooperatives and municipal utilities whose resources may be stretched thin in the event of a prolonged or aggressive cybersecurity attack.

C. Should the PSC support monitoring intelligence feeds and pushing out intelligence products for events related to Missouri?

22. Currently, in order to monitor cyber and physical security threats, the Company directly subscribes to numerous intelligence feeds, such as:

- HSIN
- E-ISAC
- Missouri Information Analysis Center ("MIAC")
- Illinois State Police ("ISP") Statewide Terrorism & Intelligence Center ("STIC")
- St. Louis Fusion Center: Terrorism Early Warning Group
- FBI Domestic Security Alliance Council ("DSAC")
- EEI Security Committee
- NERC Physical Security Advisory Group ("PSAG")
- DNG-ISAG

23. Ultimately, Ameren Missouri does not require additional assistance, particularly with regard to cybersecurity concerns. The monitoring suggested may prove more beneficial to physical security because of the inherent geographic specificity. However, as previously noted, cybersecurity threats are not subject to such boundaries, so the likelihood of a targeted cybersecurity attack in Missouri is low.

CYBER HAZARDS AND THE STATE EMERGENCY MANAGEMENT AGENCY ("SEMA") HARMONIZATION OF EMERGENCY RESPONSE PLANS IN ESF12

A. Emergency response plans harmonization

24. Pursuant to NERC reliability standards, Ameren Missouri is required to have numerous emergency plans covering various operations to ensure the reliability of the bulk power system. These plans include cybersecurity plans, and outreach to local emergency services agencies. Additional coordination and harmonization is not required.

B. Should all Missouri utilities submit updated emergency response plans on a recurring basis?

25. The emergency plans noted in the preceding paragraph are already subject to NERC and regional reliability organization scrutiny, especially during triennial audits. An additional level of oversight is unnecessary.

WHEREFORE, for the foregoing reasons, the undersigned respectfully requests that the Commission accept these comments for consideration.

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

Dated: July 5th, 2017

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 5th day of July, 2017.

/s/ *Paula N. Johnson*

ESCC
Electricity Subsector Coordinating Council

The ESCC's Cyber Mutual Assistance Program

The Electric Power Industry Shares Expertise
To Counter Cyber Attacks

Cyber Defense: Building on the Industry's Culture of Mutual Aid

The North American energy grid is a complex interconnected network of generation, transmission, and distribution systems operated by thousands of organizations. Protecting the energy grid and ensuring a reliable and affordable supply of energy are the top priorities of the electric power industry. Creating a "defense-in-depth" approach requires partnerships and coordination with the government and other critical infrastructure sectors. To coordinate security strategies with the federal government and other stakeholders, the electric power industry has created a CEO-led partnership called the Electricity Subsector Coordinating Council (ESCC).

For decades, the electric power industry has operated voluntary mutual assistance programs that work collaboratively to restore electricity following storms, earthquakes, wildfires, and other natural disasters. These mutual assistance programs provide a formal, yet flexible, process for companies to request assistance from one another.

Today, the industry's culture of mutual assistance is a model for creating responses to cyber threats to the energy grid. Based on lessons from major destructive cyber incidents overseas, and from exercises in North America, the ESCC recommended the formation of a Cyber Mutual Assistance (CMA) Program: a series of initiatives that are a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing our nation's ability to defend and protect against threats and to meet customers' expectations.

Delivering and Coordinating Cyber Mutual Assistance: How It Works

- The first initiative undertaken by the CMA Program is the creation of a Pool of industry cyber experts who are able to provide voluntary assistance to each other in the event of cyber disruptions to the energy grid.
- Participation in the Pool is open to all organizations that provide or materially support the provision of electricity.
- Participation in the Pool and response to requests for assistance made within the Pool are voluntary. There is no cost for organizations to participate in the Pool (other than the reimbursement of the expenses incurred in providing emergency cyber assistance).
- To participate in the Pool, organizations must execute a mutual non-disclosure agreement so that all participants are assured that confidential information they may share will be protected.
- Each participant in the Pool must designate one employee with appropriate cyber skills and experience, and the necessary authority, to represent the participant in the Pool (the CMA Coordinator).
- Cyber mutual assistance is intended to be advisory and short-term. It may include services, personnel, and/or equipment.

Frequently Asked Questions About Cyber Mutual Assistance

What is the Cyber Mutual Assistance Program?

The Cyber Mutual Assistance (CMA) Program refers to a series of industry initiatives developed at the direction of the ESCC to provide emergency cyber assistance within the electric power industry. The first initiative under the CMA Program is the development of a Pool of industry cyber experts who can provide voluntary assistance to other organizations in the event of a disruption to the energy grid due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of the entities participating in the CMA Program.

How can I participate in the CMA Program?

In order to participate in the CMA Program, each participating entity must (1) sign a Mutual Non-Disclosure and Use of Information Agreement, and (2) also designate a Cyber Mutual Assistance Coordinator (CMA Coordinator).

What does a CMA Coordinator do?

A CMA Coordinator is a participant's single point of contact for all matters related to the CMA Program, including the Pool. He or she is responsible for assessing his/her organization's cyber resources and responding to another participant's request for assistance, or making a request for emergency assistance on behalf of his or her company. He or she also is responsible for preparing and coordinating internal resources in connection with any assistance that his or her participating entity elects to provide.

What are the qualifications for a CMA Coordinator?

A CMA Coordinator must be a senior-level employee of a participating entity with the authority to act on behalf of the participating entity it represents. In addition, he or she must be an expert who possesses or manages sufficient cybersecurity, operating technology, and information technology skills and experience in order to be able to request, or respond to a request for, a broad range of emergency cyber needs in the context of a potentially complex and evolving cyber emergency. He or she must have sufficient understanding of the cyber functions, security, recovery processes, and available resources at his or her participating entity.

How does the Pool work?

In the event of a cyber emergency, any participant may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request to multiple or all CMA Coordinators.

What kind of assistance is provided by the Pool?

In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, and/or equipment.

For more information about the CMA Program or to become a participant, please visit www.electricitysubsector.org/CMA or contact cma@electricitysubsector.org.

April 2017