Exhibit No.:
Issue: CIP – Cyber Security
Witness: Joshua F. Phelps-Roper
Type of Exhibit: Direct Testimony
Sponsoring Party: Kansas City Power & Light Company
Case No.: ER-2016-0285
Date Testimony Prepared: July 1, 2016

MISSOURI PUBLIC SERVICE COMMISSION

CASE NO.: ER-2016-0285

DIRECT TESTIMONY

OF

JOSHUA F. PHELPS-ROPER

ON BEHALF OF

KANSAS CITY POWER & LIGHT COMPANY

Kansas City, Missouri
July 2016

" [redacted] **" Designates "Highly Confidential" Information Has Been Removed Pursuant To 4 CSR 240-2.135.**

DIRECT TESTIMONY

OF

JOSHUA F. PHELPS-ROPER

Case No. ER-2016-0285

Q: Please state your name and business address.

A: My name is Joshua F. Phelps-Roper. My business address is 1200 Main, Kansas City, Missouri 64105.

Q: By whom and in what capacity are you employed?

A: I am employed by Kansas City Power & Light Company ("KCP&L" or the "Company") as Director – NERC Implementation and Operations.

Q: On whose behalf are you testifying?

A: I am testifying on behalf of KCP&L.

Q: What are your responsibilities?

A: I am responsible for implementing projects and maintaining operational activities that ensure the Company's corporate-wide compliance with the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Cyber Security Standards. As new versions of the NERC CIP Standards are approved, I am responsible for ensuring the Company is adequately prepared to meet those standards.

Q: Please describe your education, experience and employment history.

A: I hold a Bachelors of Arts Degree in Computer Information Systems as well as a Masters of Business Administration Degree. I also hold a NERC certification as a System Operator at the Reliability Coordinator level. I have been employed by KCP&L since 2006, during which time I have held a variety of positions in Information Technology

("IT"), Generation Operations, and Project Management. Most recently, I was a project manager on KCP&L's Southwest Power Pool Integrated Marketplace implementation. I have served in my current capacity since November of 2014.

Q: Have you previously testified in a proceeding before the Missouri Public Service Commission ("Commission" or "MPSC") or before any other utility regulatory agency?

A: Yes. I previously testified before the Commission in KCP&L's last rate case, Case No. ER-2014-0370.

Q: What is the purpose of your testimony?

A: The purpose of my testimony is to describe for the Commission the nature and impact of the CIP Standards, from both an operational and financial perspective. I will describe the actual and forecasted CIP and Cyber Security costs, explain the nature of the CIP Standards including their purpose and evolution, and describe why these costs are rising rapidly with little ability for the Company to control them.

Q: What are the Company's historical and forecasted CIP and Cyber Security costs?

A: The table below describes the Company's operations and maintenance ("O&M") costs (including labor) related to CIP and Cyber Security. O&M is specifically included because the Company is only requesting forecasted rate making treatment for O&M costs.

**

[redacted]

**Total KCP&L amounts including Labor

Q: Where do the CIP Standards originate?

A: The CIP Standards are created, approved, and enforced by the Federal Energy Regulatory Commission ("FERC"), and through FERC's delegation authority by NERC. A brief history helps in understanding the FERC and NERC paradigm. FERC was granted legal authority to implement mandatory reliability standards in 2005. FERC delegated that authority to NERC, which has subsequently issued reliability standards in a variety of areas, including Cyber and Physical Security, which NERC has labeled CIP. As the Cyber and Physical Security landscape evolves, FERC issues Orders to NERC to address new or expanded threats with additional or modified CIP Standards. The CIP version 6 Standards are the latest set of approved standards meant to address the expanding Cyber and Physical Security needs of our nation's critical electric infrastructure. The CIP version 5 Standards would have become enforceable on April 1, 2016; however, FERC approved the CIP version 6 Standards which are supplanting the CIP version 5 Standards.

The CIP version 6 Standards will become enforceable on July 1, 2016. The CIP version 6 Standards have a phased implementation, meaning that some new/modified standards will be mandatorily enforceable starting on July 1, 2016, while other new/modified standards won't be mandatorily enforceable until future dates spread out over the next several years. The CIP version 6 Standards build on and expand on the CIP version 5 Standards; to illustrate the differences, my testimony will refer to the CIP version 5 and CIP version 6 standards separately to highlight the changing nature of the CIP Standards.

Under the NERC CIP version 5/6 bright line criteria, all facilities connected to or controlling the Bulk Electric System will fall under the NERC CIP Standards. This will include generating stations, substations, control centers, and other critical infrastructure. Based on where the assets fit into the bright line criteria, and also taking into account other factors NERC has defined, the assets will require varying amounts of protection, but all in-scope assets will require protection. These assets require a variety of protective measures including: physical and electronic access controls such as badging systems and protected remote access through jump hosts; logical perimeter protections such as firewalls; other logical protections such as intrusion detection systems on critical networks; new physical security protections such as pin pads in addition to badge access; enhanced personnel training; enhanced device configuration baselining and change management controls; as well as many other protective measures.

In comparison, the NERC CIP version 3 Cyber Security Standards were focused primarily in the Company's Control Centers supported by the IT division, with some work required in Transmission and Distribution ("T&D"). Under the CIP version 5 Standards, extensive work is required by IT, Generation, T&D, and Corporate (Physical)

Security. The number of in-scope facilities and Cyber Assets requiring protection is drastically expanded in CIP version 5 versus CIP version 3, and is expanded even further under CIP version 6. The types of required protective measures have also expanded in CIP version 5 and CIP version 6. CIP version 5 requirements are both broader, as seen in areas of configuration and access management, as well as more stringent, as seen in the physical and electronic access control requirements. CIP version 6 expands on CIP version 5 by adding more protections for transient cyber assets and removable media, as well as increasing the number and type of protections required for Low Impact Assets. These Low Impact Assets have a lower possible impact on the Bulk Electric System and are by far the largest group of assets under the bright line criteria; increasing protection for these assets will be costly because of their volume. In sum, the CIP version 5 and CIP version 6 Standards affect a much larger number of assets, include more types of protection, and require more stringent protections than the CIP version 3 Standards required.

Q: What is the purpose of the CIP Standards and why are they changing?

A: The purpose of the CIP Standards is to legally require electric utilities to meet mandatory levels of enhanced physical and cyber security in order to protect the Bulk Electric System. The CIP Standards mandate a broad variety of enhanced security measures to create an overall security posture intended to deter would be attackers and prevent asset destruction and/or outages.

The difficulty is that the nature of the cyber and physical threat continues to evolve, and as time goes on the threat is evolving at a faster and faster pace. As the threat evolves, security measures adequate to meet the threat put in place as little as two years

ago are no longer enough and must be enhanced. Cyber-attacks on public companies and government agencies, such as the 2015 Office of Personnel Management data breach, are a daily feature in the news.

Q: Are there recent examples of real-life attacks against electric infrastructure?

A: Yes. In late 2015, a cyber-security incident involving a United States utility was published detailing the theft of confidential and detailed information, including engineering drawings of dozens of power plants. This information would be useful in a larger cyber-attack aimed at causing an outage. Physical attacks on infrastructure, such as the 2013 attack on Pacific Gas and Electric Company's Metcalf Transmission Substation near San Jose, California, demonstrate the sophisticated nature of the threat and the possibility of real impacts to the Bulk Electric System.

Q: What have FERC and NERC done in response to these evolving threats?

A: In response to the increased risk presented by the evolving cyber and physical threats, FERC and NERC have increased the pace at which they are updating the CIP Standards. The CIP version 3 standards were approved in 2008, became enforceable in 2010, and will remain in place until July 1, 2016. In that time, the CIP version 4 standards were approved in 2012, but were sunset in 2014 due to the CIP version 5 overhaul of the CIP standards. The CIP version 5 standards were scheduled to become enforceable on April 1, 2016, but have been replaced by the CIP version 6 standards. The CIP version 6 standards, which expand the CIP version 5 standards, were approved in January 2016 and will be enforceable on July 1, 2016. CIP version 7 is being discussed within the NERC Standards Drafting Team to address outstanding issues from FERC Order 822. One specific area under discussion, and which FERC hosted a technical conference on in

January 2016, is Supply Chain Management. CIP version 3 Standards will be applicable for about 6 years when they are retired, while CIP version 4 and CIP version 5 didn't make it to enforcement before they were replaced by new CIP standards.

Q: How does this continuing evolution affect the Company's ability to forecast and manage CIP related costs?

A: The requirements and costs related to meeting the CIP Standards are evolving in several ways that make forecasting and managing the Company's CIP costs difficult. First and foremost, the increased speed of the CIP Standards revisions, as described above, makes it difficult to forecast and manage costs. Costs rise rapidly as more assets come into scope and more protections are mandated on more areas of the Company. The mandatory nature of the CIP Standards and the very real consequences of failure, both from a compliance perspective, which could include fines and/or mandated increased compliance measures, and from a security perspective, which could include outages and asset destruction, make the CIP Standards an area of high priority and a rapidly increasing cost center.

Another difficulty in forecasting costs for the CIP Standards is in interpretation of the standards. As part of the NERC standards drafting process, CIP Lessons Learned and CIP Frequently Asked Questions will be published to clarify the scope of the NERC CIP version 5 Standards. The clarifications released so far have resulted in an expansion of the Company's CIP version 5 asset list and scope versus the Company's internal evaluation of the CIP version 5 Standards. As NERC and the industry continue to provide clarifications on what the standards mean and what the Company will be held accountable for in an audit, the Company's cost to comply goes up.

In addition to the NERC interpretation guidance, it is important to understand the CIP Standards themselves require an increasing security posture as the industry evolves. For instance, right now there are various standard tests subject matter experts use to check the validity of certain cyber-security controls. These cyber-security controls ensure that a company's cyber-security posture is not reduced when changes are made to cyber systems, and are required by the CIP Standards. As time passes and technology changes, the threats become greater and more sophisticated, and more information about weaknesses in technology becomes available. In response, the cyber-security tests are changed, enhanced, or discarded in favor of something that provides more security. Even if FERC or NERC do not make any changes to the CIP Standards, the requirements of the CIP Standards still increase over time and cause costs to increase.

Finally, it is important to remember that the CIP Standards are expanding into areas of the Company that have never had to comply with NERC CIP Standards before, and that trend is continuing. The compliance workload is also increasing for areas of the Company that have previously been required to comply with CIP version 3 Standards. Forecasting costs is difficult when the Company must implement new technologies, hire new technical positions never before needed – especially when those positions are in demand across the country, and modify existing and creating new business practices in multiple divisions simultaneously. Even after the CIP version 5 and 6 go-live on July 1, 2016, stable cost data will be difficult to determine for some time. Until the Cyber and Physical Security threat landscape stabilizes, the Company and the electric industry will continue to see the CIP Standards revised and released with continued escalation of costs.

Q: Can the Company track and record all CIP and Cyber related costs?

A: Yes. The Company has developed an extensive tracking regime in order to correctly track all CIP and Cyber related costs. A common set of code blocks is being utilized across all company divisions to ensure cost tracking is straightforward and efficient. These in-scope divisions include IT, T&D, Generation, Corporate (Physical) Security, and Compliance. These costs are limited to costs directly attributable to meeting the CIP Standards or Cyber Security needs. These costs include both initial project work to implement the new CIP Standards as well as ongoing operational costs related to CIP and Cyber Security.

Additionally, the Company has in place numerous governance, project management, and cost control procedures that ensure CIP and Cyber Security efforts are efficient and cost-effective. The Company's CIP governance structure is led by Scott Heidtbrink, Chief Operating Officer, who is the executive project sponsor and the CIP Senior Manager (a position the CIP Standards require). Mr. Heidtbrink also leads the CIP Steering Committee. The CIP Steering Committee provides executive oversight of the project management organization implementing projects that ensure the Company's CIP Standards compliance. I lead the CIP implementations for the Company with the assistance of the project management organization mentioned above. The Company has divided the current CIP implementation into many sub-projects which will ensure company-wide compliance with CIP versions 5 and 6 standards on July 1, 2016 and beyond. The Company is utilizing a project management and governance structure that is common for IT related implementations and is designed to ensure our implementations are effective and costs are minimized. While the Company can minimize the costs

related to meeting the CIP Standards, it does not have a choice in implementing projects and incurring costs to meet the legally mandated CIP Standards.

Q: Does that conclude your testimony?

A: Yes, it does.

BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of Kansas City Power & Light Company's Request for Authority to Implement A General Rate Increase for Electric Service	)))	Case No. ER-2016-0285

AFFIDAVIT OF JOSHUA F. PHELPS-ROPER

STATE OF MISSOURI)
) **ss**
COUNTY OF JACKSON)

Joshua F. Phelps-Roper, being first duly sworn on his oath, states:

1. My name is Joshua F. Phelps-Roper. I work in Kansas City, Missouri, and I am employed by Kansas City Power & Light Company as Director – NERC Implementation and Operations.

2. Attached hereto and made a part hereof for all purposes is my Direct Testimony on behalf of Kansas City Power & Light Company consisting of ten (10) pages, having been prepared in written form for introduction into evidence in the above-captioned docket.

3. I have knowledge of the matters set forth therein. I hereby swear and affirm that my answers contained in the attached testimony to the questions therein propounded, including any attachments thereto, are true and accurate to the best of my knowledge, information and belief.

Joshua F. Phelps-Roper

Subscribed and sworn before me this 1st day of July, 2016.

Nicole A. Wehry
Notary Public

My commission expires: Feb. 4 2019

NICOLE A. WEHRY
Notary Public - Notary Seal
State of Missouri
Commissioned for Jackson County
My Commission Expires: February 04, 2019
Commission Number: 14391200