

FILED

SEP 22 2016

Exhibit No.: 34NP
Issue: CIP – Cyber Security
Witness: Joshua F. Phelps-Roper
Type of Exhibit: Direct Testimony
Sponsoring Party: KCP&L Greater Missouri Operations Company
Case No.: ER-2016-0156
Date Testimony Prepared: February 23, 2016

Missouri Public
Service Commission

MISSOURI PUBLIC SERVICE COMMISSION

CASE NO.: ER-2016-0156

DIRECT TESTIMONY

OF

JOSHUA F. PHELPS-ROPER

ON BEHALF OF

KCP&L GREATER MISSOURI OPERATIONS COMPANY

**Kansas City, Missouri
February 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-2016-0156

1 **Q: Please state your name and business address.**

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

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

5 A: I am employed by Kansas City Power & Light Company (“KCP&L”) as Director –
6 NERC Implementation and Operations.

7 **Q: On whose behalf are you testifying?**

8 A: I am testifying on behalf of KCP&L Greater Missouri Operations Company (“GMO” or
9 the “Company”).

10 **Q: What are your responsibilities?**

11 A: I am responsible for implementing projects that will ensure the Company’s company-
12 wide compliance with the North American Electric Reliability Corporation (“NERC”)
13 Critical Infrastructure Protection (“CIP”) version 5 Cyber Security Standards. Once the
14 NERC CIP version 5 projects are completed, I will be responsible for maintaining the
15 Company’s ongoing compliance with those standards. I will also be responsible for
16 ensuring the Company’s compliance with any future NERC CIP Cyber Security
17 Standards that are approved, such as the NERC CIP version 6 Cyber Security Standards
18 which were approved in January 2016 by the Federal Energy Regulatory Commission
19 (“FERC”).

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

2 A: I hold a Bachelors of Arts Degree in Computer Information Systems as well as a Masters
3 of Business Administration Degree. I also hold a NERC certification as a System
4 Operator at the Reliability Coordinator level. I have been employed by KCP&L since
5 2006, during which time I have held a variety of positions in Information Technology
6 (“IT”), Generation Operations, and Project Management. Most recently, I was a project
7 manager on KCP&L’s Southwest Power Pool Integrated Marketplace implementation.

8 **Q: Have you previously testified in a proceeding before the Missouri Public Service**
9 **Commission (“Commission” or “MPSC”) or before any other utility regulatory**
10 **agency?**

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

13 **Q: What is the purpose of your testimony?**

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

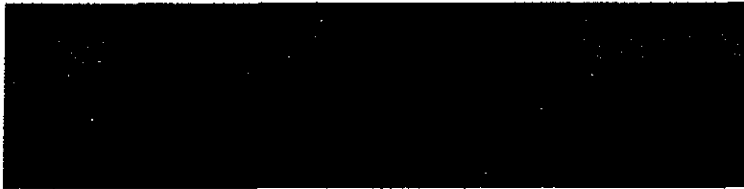
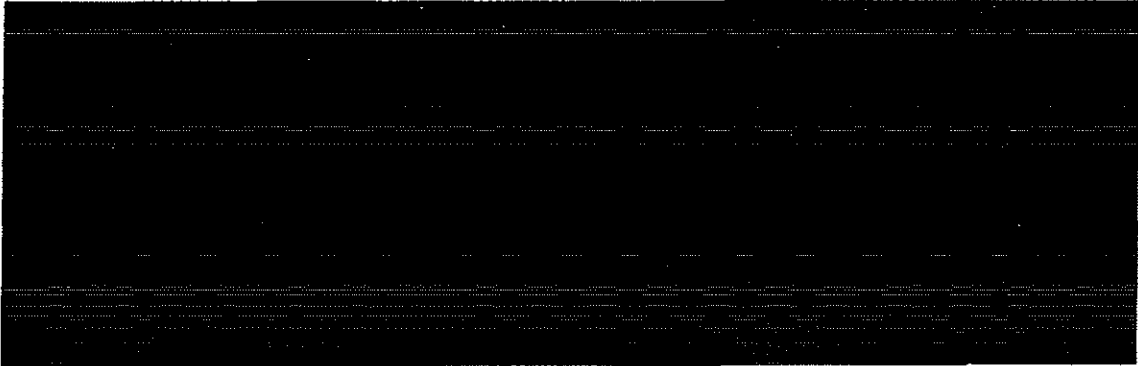
19 **Q: What are the Company’s historical and forecasted CIP and Cyber Security costs?**

20 A: The table below describes the Company’s O&M costs related to CIP and Cyber Security.
21 O&M is specifically included because the Company is only requesting forecasted rate
22 making treatment for O&M costs.

23

1

**



2

**

3 **Q: Where do the CIP Standards originate?**

4 **A:** The CIP Standards are created, approved, and enforced by FERC, and through FERC's
5 delegation authority by NERC. A brief history helps in understanding the FERC and
6 NERC paradigm. FERC was granted legal authority to implement mandatory reliability
7 standards in 2005. FERC delegated that authority to NERC, which has subsequently
8 issued reliability standards in a variety of areas, including Cyber and Physical Security,
9 which NERC has labeled CIP. As the Cyber and Physical Security landscape evolves,
10 FERC issues Orders to NERC to address those changes with additional or modified CIP
11 Standards. The CIP versions 6 Standards are the latest set of approved standards meant
12 to address the expanding Cyber and Physical Security needs of our nation's critical
13 electric infrastructure. The CIP version 5 Standards will become enforceable on April 1,
14 2016. The CIP Version 6 Standards will become enforceable in stages; the first stage

1 becomes enforceable on July 1, 2016, other stages will become enforceable over the next
2 several years.

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

15 In comparison, the NERC CIP version 3 Cyber Security Standards were focused
16 primarily in the Company's Control Centers supported by the IT division, with some
17 work required in Transmission and Distribution ("T&D"). Under the CIP version 5
18 Standards, extensive work is required by IT, Generation, T&D, and Corporate (Physical)
19 Security. The number of in-scope facilities and Cyber Assets requiring protection is
20 drastically expanded in CIP version 5 versus CIP version 3, and will expand even further
21 under CIP version 6. The types of required protective measures have also expanded in
22 CIP version 5 and CIP version 6. CIP version 5 requirements are both broader, as seen in
23 areas of configuration and access management, as well as more stringent, as seen in the

1 physical and electronic access control requirements. CIP version 6 expands on CIP
2 version 5 by adding more protections for transient cyber assets and removable media, as
3 well as increasing the number and type of protections required for Low Impact Assets.
4 These Low Impact Assets have a lower possible impact on the Bulk Electric System and
5 are by far the largest group of assets under the bright line criteria; increasing protection
6 for these assets will be costly because of their volume. In sum, the CIP version 5 and CIP
7 version 6 Standards affect a much larger number of assets, include more types of
8 protection, and require more stringent protections than the CIP version 3 Standards
9 required.

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

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

16 The difficulty is that the nature of the cyber and physical threat continues to
17 evolve, and as time goes on the threat is evolving at a faster and faster pace. As the threat
18 evolves, security measures adequate to meet the threat put in place as little as two years
19 ago are no longer enough and must be enhanced. Cyber-attacks on public companies and
20 government agencies, such as the 2015 Office of Personnel Management data breach, are
21 a daily feature in the news.

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

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

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

10 A: In response to the increased risk presented by the evolving cyber and physical threats,
11 FERC and NERC have increased the pace at which they are updating the CIP Standards.
12 The CIP version 3 standards were approved in 2008, became enforceable in 2010, and
13 will remain in place until April 1, 2016. In that time, the CIP version 4 standards were
14 approved in 2012, but were retired in 2014 due to the CIP version 5 overhaul of the CIP
15 standards. The CIP version 5 standards are scheduled to become enforceable on April 1,
16 2016. The CIP version 6 standards, which expand the CIP version 5 standards, were
17 approved in January 2016 and will supplant CIP version 5, with some new requirements
18 becoming enforceable as early as July 1, 2016. CIP version 7 is being discussed within
19 the NERC Standards Drafting Team to address outstanding issues from FERC Orders
20 706, 761, and 791. One specific area under discussion, and which FERC hosted a
21 technical conference on in January 2016, is Supply Chain Management; this is an area
22 that FERC and NERC have not issued any CIP Standards on before. CIP version 3

1 Standards will be applicable for about 6 years when they are retired, while CIP version 4
2 didn't make it to enforcement.

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

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

15 Another difficulty in forecasting costs for the CIP Standards is in interpretation of
16 the standards. NERC is publishing CIP version 5 Lessons Learned and CIP version 5
17 Frequently Asked Questions to clarify the scope of the NERC CIP version 5 Standards.
18 The clarifications released so far have resulted in an expansion of the Company's CIP
19 version 5 asset list and scope versus the Company's internal evaluation of the CIP version
20 5 Standards. As NERC continues to provide clarifications on what the standards mean
21 and what the Company will be held accountable for in an audit, the Company's cost to
22 comply goes up.

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

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

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

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

10 Additionally, the Company has in place numerous governance, project
11 management, and cost control procedures that ensure CIP and Cyber Security efforts are
12 efficient and cost-effective. The Company's CIP governance structure is led by Scott
13 Heidtbrink, Chief Operating Officer, who is the executive project sponsor and the CIP
14 Senior Manager (a position the CIP Standards require). Mr. Heidtbrink also leads the
15 CIP Steering Committee. The CIP Steering Committee provides executive oversight of
16 the project managers implementing projects ensuring the Company's CIP Standards
17 compliance. I lead the CIP implementations for the Company with the assistance of a
18 project management organization. The Company has divided the current CIP
19 implementation into many sub-projects which will ensure company-wide compliance
20 with CIP version 5 standards on April 1, 2016 and beyond. The Company is utilizing a
21 project management and governance structure that is common for IT related
22 implementations and is designed to ensure our implementations are effective and costs
23 are minimized. While the Company can minimize the costs related to meeting the CIP

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

3 **Q: Does that conclude your testimony?**

4 **A:** Yes, it does.

