

Exhibit No.:  
Issues: CIP/Cyber Security Tracker  
Witness: Randy S. Gross  
Sponsoring Party: MO PSC Staff  
Type of Exhibit: Rebuttal Testimony  
Case No.: ER-2014-0370  
Date Testimony Prepared: May 7, 2015

Filed  
June 29, 2015  
Data Center  
Missouri Public  
Service Commission

**MISSOURI PUBLIC SERVICE COMMISSION**

**REGULATORY REVIEW DIVISION**

**REBUTTAL TESTIMONY**

**OF**

**RANDY S. GROSS**

**KANSAS CITY POWER & LIGHT COMPANY**

**CASE NO. ER-2014-0370**

*Jefferson City, Missouri  
May 2015*

Staff Exhibit No. 213  
Date 6.15.15 Reporter AT  
File No. ER. 2014. 0370

**BEFORE THE PUBLIC SERVICE COMMISSION  
OF THE STATE OF MISSOURI**

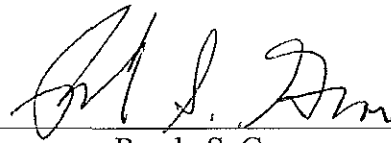
In the Matter of Kansas City Power & )  
Light Company's Request for Authority to )  
Implement a General Rate Increase for )  
Electric Service )

File No. ER-2014-0370

**AFFIDAVIT OF RANDY S. GROSS**

STATE OF MISSOURI    )  
  ) ss  
COUNTY OF COLE     )

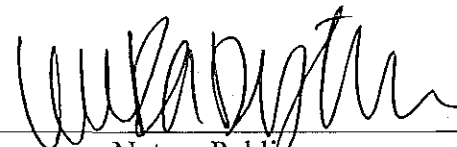
Randy S. Gross, of lawful age, on his oath states: that he has participated in the preparation of the following Rebuttal Testimony in question and answer form, consisting of 10 pages of Rebuttal Testimony to be presented in the above case, that the answers in the following Rebuttal Testimony were given by him; that he has knowledge of the matters set forth in such answers; and that such matters are true to the best of his knowledge and belief.



Randy S. Gross

Subscribed and sworn to before me this 5<sup>th</sup> day of May, 2015.

LAURA DISTLER  
Notary Public - Notary Seal  
STATE OF MISSOURI  
Commissioned for Cole County  
My Commission Expires: June 21, 2015  
Commission Number: 11203914



Notary Public

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12

**REBUTTAL TESTIMONY**

**OF**

**RANDY S. GROSS**

**KANSAS CITY POWER & LIGHT COMPANY**

**CASE NO. ER-2014-0370**

13 Q. Please state your name, position and business address.

14 A. My name is Randy S. Gross, I am a Utility Regulatory Engineer I in the  
15 Energy Unit of the Regulatory Review Division and my business address is Missouri Public  
16 Service Commission, P. O. Box 360, Jefferson City, Missouri 65102.

17 Q. Are you the same Randy S. Gross that contributed to Staff's Revenue  
18 Requirement Cost of Service Report ("COS") filed on April 2, 2015?

19 A. Yes, I am.

20 Q. What is the purpose of your rebuttal testimony?

21 A. To respond to the direct testimony of Kansas City Power & Light Company  
22 ("KCPL") witness Tim Rush and provide Staff's technical analysis of Critical Infrastructure  
23 Protection ("CIP")/Cybersecurity standards as they relate to KCPL's request for a  
24 CIP/Cybersecurity tracker.

25 Q. What does KCPL propose?

26 A. KCPL requests that a CIP tracking mechanism be authorized in this case to  
27 ensure recovery of costs necessary to address the government-mandated requirements  
28 regarding security of cyber assets essential to the reliable operation of the electric grid. The  
CIP tracker would be treated as other tracker mechanisms in Missouri.<sup>1</sup> Mr. Rush explains

---

<sup>1</sup> Direct testimony of KCPL witness Tim Rush, page 31, lines 19-23.

Rebuttal Testimony of  
Randy S. Gross

1 the regulatory framework for CIP and states that version 5<sup>2</sup> of the CIP standards contains ten  
2 new or modified standards, effective April 1, 2016<sup>3</sup>. Mr. Rush indicates that “the CIP  
3 standards represent only a portion of the Company efforts in security and cybersecurity, that  
4 “[t]he cost to comply is undetermined, but is expected to be substantial” and that the  
5 Company has committed significant resources and those efforts and resources will increase.<sup>4</sup>

6 Q. Do you agree with Mr. Rush’s characterization of the CIP Version 5 standards?

7 A. In general Staff agrees but believes there is additional information that should  
8 be considered in order to gain a more complete understanding of the CIP standards process.  
9 The CIP Version 5 standards contain three new standards and revisions to all of the previously  
10 issued version 3 standards. In 2007, the Federal Energy Regulatory Commission (“FERC”)  
11 delegated to the North America Electric Reliability Corporation (“NERC”) as the Electric  
12 Reliability Organization (“ERO”) under the authority of Section 215 of the Federal Power Act  
13 the responsibility of issuing reliability standards to address the protection of the nation’s  
14 critical infrastructure<sup>5</sup>. Version 1 took effect on July 1, 2008.<sup>6</sup> The currently enforceable  
15 version 3 standards have been in effect since October 1 of 2010. The third draft of the newest  
16 version 5 was issued on September 11, 2012, with comments and balloting due by  
17 October 10, 2012, by NERC Registered Entities. Version 5 was approved by FERC order 791  
18 on November 26, 2013, and will be enforceable on April 1, 2016.<sup>7</sup> These standards address  
19 both the cyber and physical protection of the Bulk Electric System (“BES”). The following  
20 are the currently enforceable Version 3 standards<sup>8</sup>.

---

<sup>2</sup> Version 5 is sometimes referred to as Version 5 or V5 depending on the convention used by individual sources.

<sup>3</sup> Direct testimony of KCPL witness Tim Rush, page 32, lines 2-22.

<sup>4</sup> Direct testimony of KCPL witness Tim Rush, page 33, lines 19-23.

<sup>5</sup> <http://www.nerc.com/pa/CI/Comp/Pages/default.aspx>.

<sup>6</sup> KCPL response to MOPSC data request 0467 attachment of the EnergySec CIP v5 Impact Analysis.

<sup>7</sup> Ibid.

<sup>8</sup> KCPL response to MOPSC data request 0464.

Table 1 NERC CYBER SECURITY CIP VERSION 3 STANDARDS<sup>9</sup>

CIP-002-3	Critical Cyber Asset Identification Related Information
CIP-003-3	Security Management Controls Yes Related Information
CIP-004-3a	Personnel & Training Related Information
CIP-005-3a	Electronic Security Perimeter(s)
CIP-006-3c	Physical Security of Critical Cyber Assets
CIP-007-3a	Systems Security Management
CIP-008-3	Incident Reporting and Response Planning
CIP-009-3	Recovery Plans for Critical Cyber Assets

The new Version 5 includes the following:

Table 2 NERC CYBER SECURITY CIP VERSION 5 STANDARDS<sup>10</sup>

CIP-002-5.1	BES Cyber System Categorization
CIP-003-5	Security Management Controls
CIP-004-5.1	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-5	Physical Security of Critical Cyber Assets
CIP-007-5	Systems Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-5	Recovery Plans for BES Cyber Systems
CIP-010-1	Configuration Change Management and Vulnerability Assessments
CIP-011-1	Information Protection
CIP-014-1	Physical Security

Q. How are these standards revised over time?

A. New draft versions are issued to NERC Registered Entities (including KCPL, KCPL Greater Missouri Operations Company, Ameren, Empire, etc.) for comment and voting. After comments and the voting results are received, the NERC will then utilize this information to modify the draft document to create the final version of the new standard.

The new standard is then formally issued and a later effective date is established to allow companies enough time implement them. The time between the issue and

<sup>9</sup> <http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United States>

<sup>10</sup> <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

1 implementation dates for the various revisions of the CIP standards vary based on the number  
2 and complexity of changes from the previous version and has ranged from 6 to 16 months.  
3 This entire process of issuing draft standards for comments and balloting, formally issuing the  
4 standard and then establishing a later enforcement date assures that the NERC Registered  
5 Entities are not surprised by the new standard scope and content and have enough time for  
6 effective implementation.

7 Q. What are the major differences between version 5 and the current version 3?

8 A. Both versions utilize the “defense in depth” concept and a ‘risk assessment’  
9 process but there are several significant new requirements in Version 5 including:<sup>11</sup>

- 10 • New asset identification process increases the scope of identified assets, adds  
11 three tiers of impact classification (High/Medium/Low) and uses “Bright  
12 Lines”<sup>12</sup> that simplify the criteria and reduce the ambiguity in the identification  
13 of critical assets. The critical assets now include all BES facilities and  
14 supporting systems. The previous version 3 utilized a more complicated risk  
15 based approach to identify critical assets.
- 16 • New remote access requirements and additional review and verification of  
17 personnel access privileges.
- 18 • New requirements for detection of malicious communications at the Electronic  
19 Security Perimeter (ESP)<sup>13</sup>, modified malware protection and expanded  
20 software patching requirements.
- 21 • New physical security requirements.
- 22 • Greater emphasis on security event monitoring.
- 23 • New standard for change control and configuration management.
- 24 • New standard protection of sensitive information.

---

<sup>11</sup> KCPL response to MOPSC data request 0467 attachment of the EnergySec CIP v5 Impact Analysis

<sup>12</sup> FERC Docket No. RM11-11-000; Order No. 761, Issued April 19, 2012.

<sup>13</sup> The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

1           The NERC has a Version 3 versus Version 5 compatibility table<sup>14</sup> and an  
2 Implementation Study Final Report<sup>15</sup> that are available on its website.

3           Q.     Explain the concept of “defense in depth”.

4           A.

5           “Defense in depth is the layering of security controls in such a way that the  
6 damage of an exploit is minimized. An attacker must circumvent multiple  
7 controls to exploit vulnerabilities or gain unauthorized access. Security  
8 mechanisms are also layered in such a way as to limit the damage resulting  
9 from a compromise. A medieval castle with its moats, walls and other  
10 defenses is an example of a defense in depth security stance. A well-defended  
11 castle does not rely on a single defense to protect the most valuable assets, but  
12 on multiple layers.”<sup>16</sup>

13          Q.     How does “risk assessment” affect the requirements in these standards and is  
14 there a standard process to follow?

15          A.     The NERC CIP Risk Assessment Process utilizes the National Institute of  
16 Standards and Technology (“NIST”) Special Publication 800 series to explain the content and  
17 scope of the standards<sup>17</sup>. “Because risk management is ongoing, risk assessments are  
18 conducted throughout the system development life cycle, from pre-system acquisition (i.e.,  
19 material solution analysis and technology development), through system acquisition (i.e.,  
20 engineering/manufacturing development and production/deployment), and on into  
21 sustainment (i.e., operations/support).”<sup>18</sup>

---

<sup>14</sup> <http://www.nerc.com/pa/CI/Documents/V3-V5%20Compatibility%20Tables.pdf>

<sup>15</sup> <http://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx>

<sup>16</sup> KCPL Green Impact Zone SmartGrid Demonstration Interim Technology Performance Report Version 2.0, December 31, 2013, section 2.1.2.3.3 “Defense in Depth”, page 82.

<sup>17</sup> National Institute of Standards and Technology Request for Information North American Electric Reliability Corporation Response – April 8, 2013; [http://csrc.nist.gov/cyberframework/rfi\\_comments/040813\\_nerc.pdf](http://csrc.nist.gov/cyberframework/rfi_comments/040813_nerc.pdf)

<sup>18</sup> NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments”, page ix.

Rebuttal Testimony of  
Randy S. Gross

1 Q. Mr. Rush asserts that the proposed tracking mechanism is designed to recover  
2 costs to address government-mandated requirements for cybersecurity<sup>19</sup> How does the Staff  
3 anticipate KCPL will accomplish compliance with Version 5?

4 A. The Company will identify core functional requirements and develop more  
5 specific and detailed implementation plans that will include specific activities necessary to  
6 implement these requirements. These work activities will be included in a detailed resource-  
7 loaded project schedule that will enable the creation of accurate project cost estimates. These  
8 costs estimates will include the amount of personnel required to perform the work, identify  
9 any additional equipment or software that is required, and initiate the procurement process to  
10 obtain what is required. KCPL is still in the planning process to define activities and the  
11 associated resources required for Version 5 compliance. KCPL's responses to data requests  
12 included documentation as to what it will need to accomplish for compliance.

13 Q. Can you explain what the NERC CIP V5 transition program Implementation  
14 Study Final Report is and how it can provide guidance for the transition from Version 3 to  
15 Version 5 standards?

16 A. The NERC created the CIP V5 transition program to help the industry  
17 understand the technical security requirements and help it meet the requirements timely and  
18 effectively.<sup>20</sup> The NERC conducted an Implementation Study in which six industry  
19 participants implemented elements of Version 5 in an accelerated time frame to help the ERO  
20 understand the challenges of the transition, identify guidance topics, and provide feedback, to  
21 ensure an efficient and effective transition industry-wide.<sup>21</sup> The report discusses the results of  
22 the Implementation Study and was developed in collaboration with study participants, similar

---

<sup>19</sup> Direct testimony of KCPL witness Tim Rush, page 31, lines 19-23.

<sup>20</sup> <http://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx>

<sup>21</sup> NERC Implementation Study Final Report, CIP Version 5 Transition Program, October 2014, preface.



1 to KCPL, who provided guidance as a result of their experience through their efforts to obtain  
2 compliance with Version 5<sup>22</sup>

3 Q. What observations and insights resulted from this study?

4 A. Study participants recognized the need for a structured compliance program  
5 that promotes a consistent approach across the organization. Processes need to be  
6 documented clearly and concisely, to be both readily used to protect BES Cyber Assets and to  
7 demonstrate compliance. Some participants noted the advantages in separating workflow  
8 roles, for example, by assigning different people to implement security processes from those  
9 who validate the processes.<sup>23</sup> With respect to the transition from Version 3 to Version 5<sup>24</sup>,  
10 study participants said that they were able to leverage their existing Version 3 processes to  
11 implement Version 5, but had to revise some documentation to meet the new requirements.  
12 One participant indicated that about 70 percent of their existing processes would continue to  
13 be applicable, but all of the documentation needed to be revised. Participants sometimes  
14 found it essential to involve new staff, particularly those responsible for protecting  
15 transmission and generation assets at field locations.<sup>25</sup> Study participants found it important  
16 to integrate Version 5 requirements for configuration and change management into their  
17 existing processes. Study participants with many medium-impact rating BES Cyber Systems  
18 at their transmission or generation facilities recognized that spreadsheets alone would be  
19 insufficient. Automated workflow systems provided single-source data entry and consistency

---

<sup>22</sup> Ibid. Study participants included Dayton Power & Light (DP&L), MidAmerican Energy (MidAmerican), Sacramento Municipal Utility District (SMUD), Southern Company (Southern), Tennessee Valley Authority (TVA) and Westar Energy (Westar).

<sup>23</sup> NERC Implementation Study Final Report, CIP Version 5 Transition Program, October 2014, page 5.

<sup>24</sup> Version 4 was approved but never went into effect as it was superseded by Version 5.

<sup>25</sup> Ibid

1 and easier mechanisms to support asset protection and demonstrative compliance. Study  
2 participants emphasized the need to automate.”<sup>26</sup>

3 Q. What is Staff’s understanding of where KCPL stands in the process of Version  
4 5 compliance?

5 A. Staff understands that KCPL is in the planning process stage of its compliance  
6 activities.<sup>27</sup> KCPL stated that the Version 5 implementation is a dramatic increase in the  
7 scope of critical infrastructure protection. KCPL is currently planning approximately twenty  
8 Version 5 projects involving Generation, IT, Transmission & Distribution, and Physical  
9 Security. These projects are still in the planning phase; the initial list of included employees  
10 and contractors supporting the projects will not be available until after the planning phase is  
11 completed.<sup>28</sup> KCPL provided the following information:

- 12 1. Now - 4/1/2016 – KCP&L will have ongoing activities to comply with CIP  
13 version 3
- 14 2. Now – 4/1/2016 – KCP&L will have project activities to prepare to comply  
15 with CIP version 5 high and medium requirements.
  - 16 a. By 3/13/2015 at least 4 of 20 CIP version 5 project teams will have  
17 kicked off.
  - 18 b. By 4/30/2015 all CIP version 5 project teams are forecasted to kick  
19 off.
  - 20 c. By 1/1/16 KCP&L expects to have the necessary infrastructure to  
21 be in place to be compliant with CIP version 5 high and medium  
22 requirements.
  - 23 d. By 2/15/16 KCP&L expects to complete an independent readiness  
24 evaluation of the CIP version 5 program.
  - 25 e. By 3/31/16 KCP&L expects to be fully compliant with CIP version  
26 5 high and medium requirements.
- 27 3. 4/1/2016 – CIP version 5 High and Medium requirements become  
28 enforceable and CIP version 3 requirements are retired.
- 29 4. 4/1/2016- 4/1/2017 – KCP&L will have ongoing activities to comply with  
30 CIP version 5 high and medium requirements.
- 31 5. 4/1/2016 – 4/1/2017 – KCP&L will have project activities to prepare to  
32 comply with CIP version 5 low requirements.

---

<sup>26</sup> Ibid

<sup>27</sup> Direct testimony of KCPL witness Tim Rush, page 33, lines 17-18.

<sup>28</sup> KCPL response to MOPSC data request 0461.

Rebuttal Testimony of  
Randy S. Gross

- 1           6. 4/1/2017 – CIP version 5 low requirements become enforceable.  
2           7. 4/1/2017 and beyond – KCP&L will have ongoing activities to comply  
3           with all CIP version 5 requirements<sup>29</sup>.

4           Q.     Are all these activities under the direct control of KCPL?

5           A.     Yes, as stated by KCPL in a DR response to Staff.<sup>30</sup>

6           Q.     If the proposed CIP tracker mechanism should be consistent with and similar  
7           to other tracking mechanisms used in Missouri, and all the regulated electrical utilities are  
8           subject to Version 5, are other electric utilities requesting or using such a tracking  
9           mechanism?

10          A.     Staff is not aware of any other regulated utility in the state of Missouri that has  
11          requested or is using a CIP tracking mechanism. In response to a Staff DR, KCPL stated that  
12          it was not aware of any other regulated utility in Missouri that has a CIP tracking  
13          mechanism.<sup>31</sup>

14          Q.     Has KCPL provided any projected costs or provided any additional  
15          expectations of how requested CIP tracking mechanism will be structured?

16          A.     Staff submitted several data requests to determine how KCPL is expecting the  
17          tracking mechanism to be structured and to provide any projected cost estimates. From  
18          KCPL's responses, Staff learned the following:

- 19               1. KCPL wants 100% tracking and recovery of all projected annual costs for  
20               years 2015, 2016 and 2017, and is not proposing any cap for the budgeted  
21               tracker expenses.<sup>32</sup>  
22               2. KCPL stated that the requested tracker is a two way adjustment mechanism.<sup>33</sup>

---

<sup>29</sup> KCPL response to MOPSC data request 0465.

<sup>30</sup> KCPL response to MOPSC data request 0459.

<sup>31</sup> KCPL response to MOPSC data request 0468.

<sup>32</sup> KCPL response to MOPSC data requests 0459 and 0471.

<sup>33</sup> KCPL response to MOPSC data request 0469.

Rebuttal Testimony of  
Randy S. Gross

1 “The CIP/Cyber Tracker is for incremental O&M dollars, labor &  
2 non-labor, spent to meet regulatory requirements for protection of  
3 critical infrastructure, inclusive of NERC, DOE, NRC, etc., or  
4 Cyber Security needs. The tracker would include amounts for Non-  
5 Labor O&M in future years which are incremental to what was  
6 spent in the test year. The tracker would include incremental  
7 employee costs beyond the headcount in place at KCP&L for CIP  
8 and Cyber Security purposes on May 31, 2015.”<sup>34</sup> “The CIP  
9 forecast is based on NERC CIP standards which are already subject  
10 to enforcement and NERC CIP standards approved and subject to  
11 future enforcement. Projected costs are based on project planning  
12 for CIP version 5 which is still in process.”<sup>35</sup>

13 Staff’s understanding is that KCPL is proposing that all costs to ensure compliance  
14 with both current Version 3 standards and all costs required to obtain and maintain  
15 compliance with Version 5 standards be included within the tracker.

16 Q. What is Staff’s position regarding KCPL’s proposed CIP/cybersecurity  
17 tracker?

18 A. As discussed in the rebuttal testimony of Staff witnesses Karen Lyons and  
19 Mark L. Oligschlaeger, Staff recommends that this tracker not be authorized.

20 Q. Does this conclude your rebuttal testimony?

21 A. Yes, it does.

---

<sup>34</sup> KCPL response to MOPSC data request 0466.

<sup>35</sup> Ibid.