Exhibit No.:	
Issue:	Data Privacy/Security
Witness:	Gary Johnson
Type of Exhibit:	Rebuttal Testimony
Sponsoring Party:	Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company
Case Nos.:	ER-2018-0145 and ER-2018-0146
Date Testimony Prepared:	July 27, 2018

MISSOURI PUBLIC SERVICE COMMISSION

CASE NOS.: ER-2018-0145 and ER-2018-0146

REBUTTAL TESTIMONY

OF

GARY JOHNSON

ON BEHALF OF

KANSAS CITY POWER & LIGHT COMPANY and
KCP&L GREATER MISSOURI OPERATIONS COMPANY

Kansas City, Missouri
July 2018

REBUTTAL TESTIMONY

OF

GARY JOHNSON

Case Nos. ER-2018-0145 and ER-2018-0146

Q: Please state your name and business address.

A: My name is Gary Johnson. 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") as Senior Director Infrastructure and Cyber Security.

Q: On whose behalf are you testifying?

A: I am testifying on behalf of KCP&L and KCP&L Greater Missouri Operations Company ("GMO") (collectively, the "Company").

Q: What are your responsibilities?

A: My responsibilities include Cybersecurity, Physical Security and IT Infrastructure (data centers, network, storage, computing help desk, asset management, etc.).

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

A: I studied Information Systems at Potomac College in Rockville, MD. I am a US Army veteran with over 30 years of Information Technology experience. I have been in my current role at KCP&L since December of 2015. Prior to that I was the VP of Security at Cerner Corporation from 2010-2015 and the VP of IT Infrastructure also at Cerner Corporation from 2005-2010.

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

A: No.

Q: What is the purpose of your testimony?

A: I will respond to some of the issues raised in the direct testimony of OPC witness Geoff Marke.

Q: How does the Company stay current on cybersecurity issues?

A: The Company participates in NESCO (National Electric Sector Cybersecurity Organization), Fusion Centers, US-CERT (US Computer Emergency Readiness Team), ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), EPRI (Electric Power Research Institute), EEI (Edison Electric Institute), CIPWG (Critical Infrastructure Protection Working Group), Transmission Forum Security Practices Group, ISSA (Information Systems Security Association), ISC2 (International Information System Security Certification Consortium), ISACA (Information Systems Audit and Control Association), E-ISAC (Electricity Information Sharing and Analysis Center), NERC (North American Electric Reliability Corporation), CIPC (Companies and Intellectual Property Commission), RTO Compliance Forum and MISO Compliance Forum.

Q: How does the Company protect customer information?

A: The Company has a strong commitment to protecting customer information including customer usage information. The Company protects the entire enterprise's information, including customer information, with the same protections. These protections include:

- Traffic coming in from the internet is inspected for denial of service (DOS) attacks by our DOS appliance and cloud service. If a DOS attack is detected the cloud service blocks the DOS in the Internet before it reaches the Company network.
- Network firewalls are in place to help manage access and to prevent malicious traffic from entering the enterprise. These firewalls also have web filtering to stop traffic from malicious websites and intrusion detection and prevention capabilities that help prevent advanced threats that make it past typical firewall packet inspection. The Company also has deployed additional intrusion detection monitoring in order to have layers of intrusion detection from different manufacturers.
- Web application firewalls (WAF) are in place to help prevent application-specific threats. WAF's protect against common attacks such as cross site scripting (XSS) and SQL injection. These and other attacks typically take advantage of vulnerabilities in application code.
- Restricted user access on servers prevents attackers from running commands as non-privileged users. This is part of role-based access, commands and capabilities are assigned at a role level. This is designed to ensure that only those users that need to run commands or have access are those that have it.
- Application whitelisting prevents unknown executables from running, preventing ransomware, other malicious, or unapproved software from running. There is no malware that can run on a white-listed machine. Only

those utilities and applications that are authorized (white-listed) can execute.

- The entire enterprise is scanned continuously for vulnerabilities. If found, vulnerabilities are then evaluated for applicability and remediated or mitigated.
- Code scanning detects defects and vulnerabilities in the application code that could allow attackers to execute malicious requests. Code is scanned before implementation and defects or vulnerabilities are mitigated or remediated before going into production.
- Database-level protections prevent unauthorized commands from being run against the database. This works in much the same way as a WAF and protects the database against database specific attacks.
- Customer's personally identifiable information (PII) is encrypted while on the Company's system. Only authorized users can view unredacted PII.
- The Cyber Threat Operations Center (CTOC) is monitoring and responding to security events on a 24X7 basis.
- The Cyber Incident Response Team is available to react to events escalated from the CTOC on a 24X7 basis.

Q: Witness Marke proposes that the Commission should order the Company to prepare an annual cybersecurity plan and privacy impact assessments. What is your reaction to this proposal?

A: The risk that the CSP (Cybersecurity Plan) would be disclosed to those that could use it to do harm to the Company is high enough that the plan would have to be at such a high level

that it wouldn't provide much value. A better approach would be closed door meetings with the Commission to discuss the plan, results of any assessments and action plans accordingly. The Company already conducts third party audits of its cybersecurity practices against NIST Cybersecurity Framework standards but has not conducted specific PIA's (Privacy Impact Assessments). The Company already has a data breach notification plan and our privacy policy is posted on the company website.

Q: Should the Commission adopt OPC's other recommendations in this case?

No. OPC's recommendations need to be vetted among stakeholders including those that are not parties to this rate case. For example, while there are Green Button standards and guidelines, clarification of specific asks for all utilities in Missouri would provide uniform direction for Missouri customers and allow the utilities to work to a common set of regulatory expectations.

Today, KCP&L provides download data for customers in the following formats:

- Monthly data downloads for up to 25 months
- Daily data downloads for 3 billing periods

While these capabilities do not match up directly to the Green Button Initiative, the Company is committed to providing customer access to detailed data. The recent implementation of the One CIS project included a new billing platform with access to interval data from an advanced meter data management platform and enables the capability to provide greater user access to historical data. The Company is currently considering implementing the Green Button in a future phase of the billing system.

Mr. Marke is correct that it is incumbent on the utility to protect the customers' data. To ensure that happens, customer protection criteria must be specified for third parties

to adhere to prior to gaining access to customer data. The utilities will have no control over treatment of the customers data once the third party has access.

Company witness Ives also addresses the problems associated with addressing OPC's industry-wide recommendations in the rate case of a single utility.

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-2018-0145
In the Matter of KCP&L Greater Missouri Operations Company's Request for Authority to Implement A General Rate Increase for Electric Service	))))	Case No. ER-2018-0146

AFFIDAVIT OF GARY JOHNSON

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

Gary Johnson, being first duly sworn on his oath, states:

1. My name is Gary Johnson. I work in Kansas City, Missouri, and I am employed by Kansas City Power & Light Company as Senior Director Infrastructure and Cyber Security.

2. Attached hereto and made a part hereof for all purposes is my Rebuttal Testimony on behalf of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company consisting of _____ (__) 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

Gary Johnson

Subscribed and sworn before me this _____ day of July 2018.

Notary Public

My commission expires: 4/26/2021

ANTHONY R WESTENKIRCHNER
Notary Public, Notary Seal
State of Missouri
Platte County
Commission # 17279952
My Commission Expires April 26, 2021