Exhibit No.:	_____
Issue(s):	Privacy and cybersecurity implications with the advancement of the smart grid/ Customer data breaches/ Commission rules regarding privacy/ Applicable laws and practices in other states/ OPC recommendations
Witness/Type of Exhibit:	Marke/Direct
Sponsoring Party:	Public Counsel
Case No.:	ER-2018-0145 and ER-2018-0146

DIRECT TESTIMONY

OF

GEOFF MARKE

Submitted on Behalf of
the Office of the Public Counsel

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

Case No. ER-2018-0145 and ER-2018-0146

June 19, 2018

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-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	))))	File No. ER-2018-0146

AFFIDAVIT OF GEOFF MARKE

STATE OF MISSOURI)
) ss
COUNTY OF COLE)

Geoff Marke, of lawful age and being first duly sworn, deposes and states:

1. My name is Geoff Marke. I am a Regulatory Economist for the Office of the Public Counsel.

2. Attached hereto and made a part hereof for all purposes is my direct testimony.

3. I hereby swear and affirm that my statements contained in the attached testimony are true and correct to the best of my knowledge and belief.

Geoff Marke
Chief Economist

Subscribed and sworn to me this 19th day of June 2018.

NOTARY PUBLIC NOTARY SEAL STATE OF MISSOURI

JERENE A. BUCKMAN
My Commission Expires
August 23, 2021
Cole County
Commission #13754037

Jerene A. Buckman
Notary Public

My commission expires August 23, 2021.

TABLE OF CONTENTS

DIRECT TESTIMONY

OF

GEOFF MARKE

KANSAS CITY POWER & LIGHT COMPANY
CASE NO. ER-2018-0145

I. INTRODUCTION

Q. Please state your name, title and business address.

A. Geoffrey Marke, PhD, Chief Economist, Office of the Public Counsel ("OPC"), P.O. Box 2230, Jefferson City, Missouri 65102.

Q. What are your qualifications and experience?

A. I have been in my present position with OPC since 2014 where I am responsible for economic analysis and policy research in electric, gas and water utility operations.

Q. Have you testified previously before the Missouri Public Service Commission?

A. Yes. A listing of the cases in which I have previously filed testimony and/or comments before the Commission is attached in Schedule GM-1.

Q. What is the purpose of your direct testimony?

A. The purpose of this testimony is to propose certain preliminary privacy standards and safeguards for KCPL and GMO ratepayers regarding customer data and advanced metering infrastructure ("AMI" or "smart meter"). OPC recommends that the Commission order KCPL and GMO to adopt these basic privacy standards and safeguards and to open a rulemaking workshop to explore more robust consumer protection and include needed codified language regarding data privacy and information sharing in its Chapter 13 – Service and Billing Practices for Residential Customers of Electric, Gas, Sewer, and Water Utilities and complementary affiliate transaction rules found in Chapter 20.

I provide information and recommendations on the following:

- An overview of the privacy and cybersecurity implications that accompany the transition into two-way, real-time, energy consumption and customer information data that AMI and the "smart grid" enables;
- Illustrative examples of customer data and confidentiality breaches;
- A review of the current Commission rules regarding customer data, privacy and information sharing;
- Applicable privacy laws and practices by other State Regulatory Commissions; and
- OPC's specific recommendations for the Commission's consideration including: privacy plans, consent, disclosure, breach protocols and implementation of the Green Button software.

II. PRIVACY AND CYBERSECURITY IMPLICATIONS WITH THE ADVANCEMENT OF THE SMART GRID

Q. What is advanced metering infrastructure?

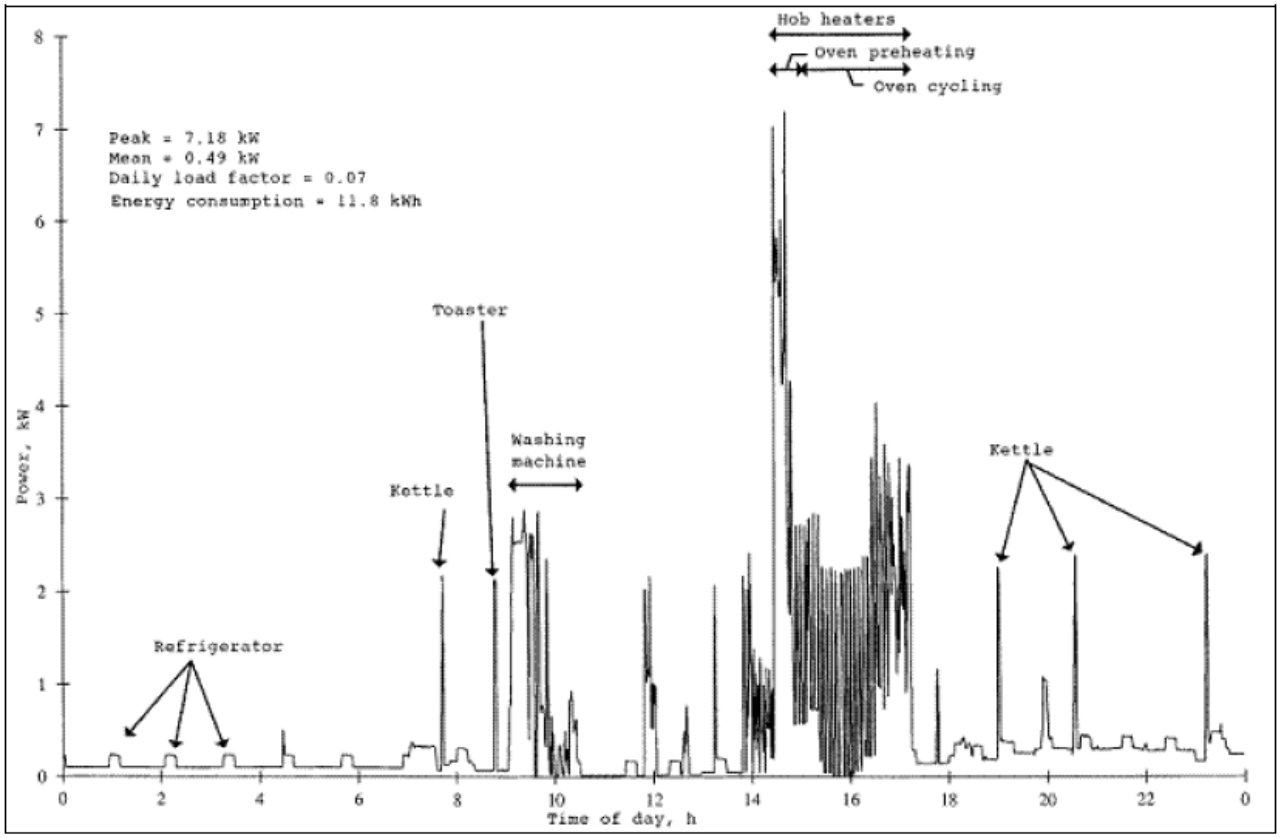
A. Advanced metering infrastructure ("AMI") is an integrated system of smart meters, communication networks, and data management systems that enables two-way communication between utilities and customers. The system provides a number of functions that were not previously possible or that had to be performed manually, functions such as the ability to automatically and remotely measure electricity use, connect and disconnect service, detect tampering, identify and isolate outages, and monitor voltage.

Combined with "smart appliances," such as programmable thermostats or water heaters, AMI also enables utilities to offer new time-based rate programs that encourage customers to reduce peak demand and manage energy consumption. In theory, AMI should reduce costs for metering and billing, and lower utility capital expenditures and outage costs.

Q. Are there any potential liabilities associated with AMI?

A. Yes. AMI will also greatly expand the amount of data that can be monitored, collected, aggregated, and analyzed. This expanded information promotes opportunities for efficiencies, but also increases privacy and potential exploitation concerns. For example, specific appliances and generators may potentially be identified from the signatures they exhibit in electric information at the meter when collections occur with greater frequency, unlike traditional monthly meter readings that occur once an hour or less frequently. Figure 1, developed by the National Institute of Standards and Technology ("NIST"), shows how AMI meter data can be used to decipher the activities of a home's occupants by matching data on their electricity usage with known appliance load signatures.

Figure 1: Identification of household activities from electricity usage data[1]



[1] National Institute of Standards and Technology (2010) Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid 13 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

It is reasonable to assume that customers understand utility companies must collect usage data to bill them based on that usage. Customers receive their statements each month demonstrating this fact. However, most customers are probably not familiar with the sophistication of smart meters and the detailed data sets that can be derived from them. Even if customers are aware their utility usage can be recorded in sub-fifteen minute intervals, a reasonable customer would probably be surprised, if not shocked, to know that data from smart meters can potentially be used to pinpoint the usage of specific appliances.

Detailed electricity usage data offers a window into the lives of people inside of a home, and the transmission of the data potentially subjects this information to third party interception, theft or exploitation. According to the Department of Energy, smart meters may be able to reveal occupants' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment, such as plasma TVs, and whether they use certain types of medical equipment.[2] Data that reveals which appliances a person is using could permit health insurance companies to determine whether a household uses certain medical devices, and appliance manufacturers to establish warranty violations. Marketers could use it to make targeted advertisements. Criminals could use it to time a burglary and figure out which appliances they would like to steal. If a consumer owned a plug-in electric vehicle, data about where the vehicle has been charged could permit someone to identify the consumer's location and travel history. There are also fourth amendment questions surrounding the access of this level of information for law enforcement personnel.

According to the Electronic Privacy Information Center ("EPIC"), the faith placed in the capacity of the Smart Grid to safeguard sensitive personal information is unfounded. "An attacker with $500 of equipment and materials and a background in electronics and

[2] Department of Energy (2010) Data access and privacy issues related to smart grid technologies 5,9. https://www.energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf

software engineering could take command and control of the [AMI] allowing for the *en masse* manipulation of service to homes and businesses." Therefore, it is possible that "just as identities, credit and debit card numbers, and other financial information are routinely harvested and put up for sale on the Internet, so can Smart Grid identifiers and related information."[3]

Q. Are there other privacy concerns beyond detailed energy usage that potentially could be compromised in a data breach?

A. Yes, detailed energy usage is just one of the potential data elements present within the smart grid that could impact privacy if not properly safeguarded. Table 1 is reprinted from NIST: Guidelines for Smart Grid Cybersecurity which identifies and describes potential personal information embedded within the smart grid that could compromise a consumer's privacy.

Table 1: Reprint of NIST information potentially available through the smart grid[4]

Data Elements	Description
Name	Party responsible for the account
Address	Location where service is being taken
Account Number	Energy consumption recorded between 15-60 minute intervals
Financial information	Current or past meter reads, bills and balances available, including history of late payments/failure to pay, if any
Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used

[3] Coney, L. (2010) Electronic Privacy Information Center. Smart Grid Summit: Privacy perspective on protecting the grid and consumer data. https://epic.org/privacy/smartgrid/EPIC_Statement_Smart_Grid_Summit_Cybersecurity_and_Privacy.pdf

[4] National Institute of Standards and Technology (2014) Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid 13 NISTIR 7628 Revision .1 https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

Distributed resources	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
Meter IP	The Internet Protocol address for the meter, if applicable

Q. Are third-party contractors to a utility susceptible to data breaches?

A. Yes. Every time a utility contracts with a third-party the level of complexity and privacy concerns are amplified, as additional opportunities for data breaches can occur. Consumer data moving through a smart gird becomes stored in many locations, both within the grid and within the physical world. Thus, because the data is widely dispersed, it becomes more vulnerable to interception by unauthorized parties and to accidental breach. The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network—or through communications components that may be incompatible with one another or possess outdated security protections. Thus, robust safeguards need to be in place not only for the utility, but also with each and every one of its third-party contractors, sub-contractors and affiliates who have access to the data. Many of the most high-profile data breaches were the result of inadequate safeguards by third-party entities. However, the financial and reputational damage is almost assuredly disproportionally borne by the principal.

III. CUSTOMER DATA BREACHES

Q. Could you provide some illustrative examples of data breaches?

A. Yes. Table 2 provides a breakdown of ten high-profile data breaches, including the scale and highlighted features of the breach.

Table 2: Illustrative list of large-scale data breaches

Organization	Scale	Highlights
Anthem	78.8 million users	The hack began in February 2014 when just one user at an Anthem subsidiary opened a phishing email that gave the hacker access to Anthem's data warehouse. [5]
Target	110 million users	Target was affected following the initial breach of a third-party vendor, Fazio Mechanical Services, most likely through a phishing operation. Following the penetration of the Target network, weak spots were pinpointed, sensitive data was compromised, and the hackers constructed a bridge within Target's own systems to transfer the sensitive data out. [6]
Yahoo	3 billion users	The stolen data has been found all over the dark web, and worst yet, being sold to the highest bidder. Yahoo waited four years to finally disclose this breach, following its sale to Verizon. Russian hackers are believed to be the culprits, but no one is sure how they gained access to Yahoo's systems.[7]
eBay	145 million users	The hackers accessed a database that held names, email addresses, birth dates, encrypted passwords, physical addresses and phone numbers. Hackers had access to eBay's corporate network for 229 days. [8]
Equifax	146.6 million users	More than 99% of affected consumers had their social security numbers exposed (145.5 million people). More than 200,000 credit card numbers and expiration dates were also compromised, as well as government-issued identification documents – like driver's licenses, taxpayer ID cards, passports and military IDs – for 182,000 consumers. The hole that the breach broke through was revealed in March 2017, but Equifax failed to address it, and the subsequent breach was discovered in July 2017. It was made public on September 7, 2017. [9]

[5] Mukherjee,S (2017) Anthem's historic 2015 health records breach was likely ordered by a foreign government. *Fortune*. http://fortune.com/2017/01/09/anthem-cyber-attack-foreign-government/
[6] Ciambrone, A. et al. (2017) Breaking the Target: An analysis of Target data breach and lessons learned. *IEEE*. https://arxiv.org/pdf/1701.04940.pdf
[7] Larson, S. (2017) Every single Yahoo account was hacked-3 billion in all. *CNN Money*. http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html
[8] Perlroth, N. (2014) eBay urges new passwords after breach. *NY Times*. https://www.nytimes.com/2014/05/22/technology/ebay-reports-attack-on-its-computer-network.html
[9] Johnson, A. (2018) Equifax breaks down just how bad last year's data breach was. *NBC News*. https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496

Uber	20 million users & 600,000 drivers	Uber waited over a year to disclose the breach, and also paid the attackers $100,000 to delete the data and keep the breach quite. Uber never confirmed that the data was, in fact, destroyed. [10]
US Office of Public Management	22 million users	Chinese hackers were able to access the system as far back as 2012, and it wasn't discovered until 2014. It is believed that his hack may have jeopardized "an entire generation of national security." [11]
Sony PlayStation	77 million users	Sony was forced to shut down their online gaming/media network for almost an entire month in order to secure the breach. Not only was sensitive date released, but the network itself was left inoperable to its users and administration. [12]
TJX	94 million users	Hackers gained access to a decryption tool that allowed them to "skim" data during payment card approval process. Hackers also gained access to the system by using job application kiosks in Marshall's Department stores. [13]
Heartland Payment Systems	134 million users	Heartland had no incident response plan in place, and because of an overall out-of-compliance security plan, they were barred from making any transactions through Visa or MasterCard until May 2009.[14]

Q. Are there any germane examples involving electric utilities?

A. Yes. A simple Google search for "utility data breach" will populate many examples, but, most recently, the breach of TIO Networks, a subsidiary of PayPal, and a third-party payment processor contractor for many utilities nationwide was compromised. Impacted

[10] Newcomer, E & T. Shields (2018) Uber's 2016 breach affected more than 20 million U.S. users. *Bloomberg News*. https://www.bloomberg.com/news/articles/2018-04-12/uber-breach-exposed-names-emails-of-more-than-20-million-users

[11] Koerner, B. (2016) Inside the cyberattack that shocked the US government. *Wired*. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[12] Gaudiosi, J. (2014) Why Sony didn't learn from its 2011 hack. *Fortune*. http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/

[13] Vennamaneni, M. (2016) Security breach at TJX—Analysis. *Medium*. https://medium.com/@mounicav/security-breach-at-tjx-analysis-675a0fb1cedf

[14] Secureworks (2012) A famous data security breach & PCI case study: four years later. *Securworks*. https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland

utilities included KCPL,[15] Duke Energy,[16] Avangrid[17] Springfield City Utilities (Missouri),[18] and PSE&G.[19]

Another high profile utility data breach occurred in 2012 when New York State Electric & Gas Corporation ("NYSEG") and Rochester Gas and Electric Corporation ("RG&E") ratepayers private information was compromised through a subcontractor. As a result, confidential information including Social Security Numbers, dates of birth, and in some cases, financial institution account information was exposed. Schedule GM-2 includes the New York Public Service Commission's Order and the New York Commission Staff's investigative report on this breach in Case No. 12-M-2082. According to the New York Public Service Commission's press release:

> "Our investigation found that NYSEG and RG&E failed to meet industry standards and best practices to protect personally identifiable information of customers," said Commission Chairman Garry Brown. "As a result, we are directing the companies to immediately take action to address the vulnerabilities on its computer billing and records systems currently used to take and maintain confidential customer information." . . .
>
> Based upon the investigation's findings, the companies should further refine policies, processes and procedures regarding confidentiality safeguards. The companies should minimize access to the most sensitive personally identifiable information by maintaining a strictly "need to know" standard for contractors and

[15] KCPL (2017) Potential data breach at authorized payment locations. *KCPL*. https://www.kcpl.com/involvement/safety/fraud-alerts/potential-data-breach-at-authorized-payment-locations
[16] Roberts, D. (2017) Duke Energy says data breach may have exposed personal information for many customers. *Charlotte Observer*. http://www.charlotteobserver.com/news/business/article188108864.htm
[17] Turmelle, L. (2017) Hacking of Conneticut utility company exposes as many as 52,000 customers information. *New Haven Register*. http://www.govtech.com/security/Hacking-of-Connecticut-Utility-Company-Exposes-As-Many-As-52000-Customers-Information.html
[18] Pyatt, C. (2017) City Utilities discloses possible data breach. *Fox 5 KRBK*. http://www.fox5krbk.com/story/36974808/city-utilities-discloses-possible-data-breach
[19] Goldman, J. (2017) PSE&G customers exposed to data breach through Paypal subsidiary. *NJ Advance Media*. http://www.nj.com/business/index.ssf/2017/12/data_breach_could_affect_some_pseg_customers.html

employees alike. The companies should conduct, at least annually, an incident response exercise simulating a breach of such data. The companies should establish a protocol for notification of regulators in the event of any significant cyber incident involving a possible compromise of customer data; and the companies should promptly implement steps to ensure the security of all data stored on company mobile computers and removable data storage media. . .

In addition to the foregoing recommendations, the Commission raised concerns that the issue of costs that both the companies incur in responding to this security breach. The Commission will require the companies segregate and report all of the costs associated with rectifying the security breach, including the customer care costs identified above as well as any incremental investigation and remediation costs, as part of respective 2012 earnings sharing filings, and that the Commission closely scrutinize any proposal to incorporate these costs in the earnings sharing calculation. In this way, the companies will be put on notice that they will be required to justify fully the inclusion of any such expenses in their earnings sharing calculations.[20]

IV. COMMISSION RULES REGARDING PRIVACY

Q. Does this Commission have rules in place to safeguard utility customer privacy?

A. No. A word search through the Commission's 400+ pages of rules only contain the word "privacy" twice and in both instances it was in the context of telecom. The first instance can be found in 4 CSR 240-29.060 Enhanced Record Exchange Rules:

> Special Privacy Provisions for End Users Who Block Their Originating Telephone Number

And the second in in 4 CSR-31.130 (7) Universal Service Rules:

[20] Platsky, J. (2012) Regulators criticize NYSEG for computer security breach. http://www.thecre.com/fisma/?p=2145

> A statement that the applicant will satisfy applicable consumer protection, consumer privacy, and service quality standards. This statement shall include a list of those specific standards the applicant deems applicable. A wireless applicant shall include a statement that it will comply with the Cellular Telecommunications and Internet Association's Consumer Code for Wireless Service;

No such language could be found for rules governing electric, natural gas and water services.

Q. Do the Commission's Chapter 13: "Service and Billing" Rules contain any provision regarding customer information or data privacy?

A. None. The Commission's billing rules contain no language regarding data privacy, data ownership or data access. On the contrary, a large section of these rules focus on estimating monthly or quarterly bills when no meter or improperly calibrated meters are in place. This clearly reflects a different regulatory reality as this is literally the exact opposite problem that OPC is concerned with.

Q. Do any of the Commission rules reference the utility sharing of customer information?

A. Yes. Both the electric and gas utilities have affiliate transactions rules in place that state:[21]

> Specific customer information shall be made available to affiliated or unaffiliated entities only upon consent of the customer or as otherwise provided by law or commission rules or orders. General or aggregated customer information shall be made available to affiliated or unaffiliated entities upon similar terms and conditions. The regulated electrical corporation may set reasonable charges for costs incurred in producing customer information. Customer information includes information provided to the regulated utility by affiliated or unaffiliated entities.[22]

[21] There are no affiliate transactions rules for water utilities in Missouri. It is also worth noting that Missouri American Water, is now the second utility (and one of the first water utilities in the nation) to begin deployment of AMIs in its service territory.

[22] 4 CSR 240-20.015(2)(C) & 4 CSR 240-40.015 (2)(C)

That being said, it is not entirely clear what "customer information" includes and whether or not that would extend to energy usage information. It is also not clear what is meant by "general or aggregated information." No threshold or standard is given.

Presently, these rules reflect a regulatory era that is quickly eroding as data analytics and supportive smart infrastructure is increasingly deployed. Today, at best, the rules are inadequate. Moving forward, the threat to consumers will only increase without proper safeguards, policies, practices, and agreed-to regulatory rules and oversight in place.

As it stands, Missouri utility billing and associated practices related to customer data privacy is already lagging behind other states. A 2016 National Regulatory Research Institute ("NRRI") white paper, "Energy and Water Utility Billing Rules, Standards, and Practices: A Survey of the State of the Art and Ideas about Future Directions"[23] listed 16 separate billing rule categories and/or adopted best practices including customer data privacy. The NRRI determined that Missouri only had minimal rules or adopted practices in 9 of the 16 listed categories; on the other hand, 19 states had active policy in place regarding customer data privacy back in 2016. [24]

IV. APPLICABLE LAWS AND PRACTICES IN OTHER STATES

Q. Are there any applicable federal laws that provide privacy protections for smart grid technologies?

A. According to the 2014 NIST: Guidelines for Smart Grid Cybersecurity, U.S. federal privacy laws cover a wide range of industries and topics. However, it is not clear to what extent current federal laws that provide privacy protections may apply, if at all, to consumer energy usage

[23] Stanton T. & K. Kline (2016) Energy and water utility billing rules, standards, and practices: A survey of the state of the art and ideas about future directions. Report No. 16-03http://nrri.org/research-papers/
[24] Billing categories listed included: minimum contents, service deposits, estimated bills, master meters, historical usage, dispute resolution, third-party agents, levelized billing, payment methods, payment assistance, partial payments, special payment plans, denial and/or disconnection, weather-related shutoff, electronic billing, and customer data privacy.

data that may be possible by advanced smart grid technologies and identification techniques. NIST identifies the following applicable federal privacy laws in various disciplines or sectors:

Healthcare: Includes the Health Insurance Portability and Accountability Act ("HIPAA") and the associated Health Information Technology for Economic and Clinical Health ("HITECH") Act.

Financial: Examples include the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and the Red Flags Rule.

Education: Examples include the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).

Communications: Examples include the First Amendment to the U.S. Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA).

Government: Examples include the Privacy Act of 1974, the Computer Security Act of 1987, and the E-Government Act of 2002.

Online Activities: Examples include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, commonly known as the "Patriot Act").

Privacy in the Home: Examples are the protections provided by the Fourth and Fourteenth Amendments to the U.S. Constitution.

Employee and Labor Laws: Examples include the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity (EEO) Act.

General Business and Commerce: One example is Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices, and has been used by the FTC to cover a wide variety of businesses.[25]

Q. Are there any States that have enacted privacy protection laws specific to smart grid technologies?

A. Again according to the NIST Report, there were at least seven States with smart-grid specific privacy protection laws in place in 2014.

California Senate Bill 1476: customer data generated by smart meters is private and can only be shared with third parties upon consent of the customer, with the following exceptions: for basic utility purposes, at the direction of the California PUC, or to utility contractors implementing demand response, energy efficiency or energy management programs;

Illinois S.B. 1652: Develop and implement an advanced smart grid metering deployment plan, which included the creation of a Smart Grid Advisory Council and H.B. 3036 amended the smart grid infrastructure investment program and the Smart Grid Advisory Council;

Maine H.B. 563: directed the Public Utility Commission to investigate current cybersecurity and privacy issues related to smart meters;

New Hampshire S.B. 266: prohibition on utility installation of smart meters without the property owners' consent. Utilities must disclose in writing the installation of a smart meter;

Ohio S.B. 315: encourages innovation and market access for cost effective smart grid programs and H.B. 331 – creates a Cybersecurity, Education and Economic Development Council to help improve state infrastructure for cybersecurity;

[25] National Institute of Standards and Technology (2014) Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid 13 NISTIR 7628 Revision .1 https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

Oklahoma Law H.B. 1079: established the Electronic Usage Data Protection Act that directs utilities to provide customers with access to and protection of smart grid consumer data;

Vermont S.B. 78: promote statewide smart grid deployment and S.B. 214/Act 170 directs the Public Utility Board to set terms and conditions for access to wireless smart meters. The law also requires consumer's written consent prior to smart meter installation and requires removal of smart meters upon request/cost-free opt-out of Smart Meters.[26]

OPC is currently reviewing other States to see if this list needs to be updated. We are aware that the District of Columbia and two additional states have put statutes in place since the NIST report was published: 1) the District of Columbia passed H.B. 1896 and H.B. 2264 which includes customer consent to release data, specific definitions for intended purpose, affirmation of customer consent for release of data for secondary purposes, a resolution process for customer complaints related to unlawful disclosure of data and third-party contract requirements related to disclosure of data; 2) New Jersey § 48:3-85(b) which provides a general data protection statute applicable to smart gird interval data; and Washington, WAC 480-100-153 which states:

Disclosure of private information

(1) An electric utility may not disclose or sell private consumer information with or to its affiliates, subsidiaries, or any other third party for the purposes of marketing services or product offerings to a customer who does not already subscribe to that service or product, unless the utility has first obtained the customer's written permission to do so.

(2) Private consumer information includes the customer's name, address, telephone number, and any other personally identifying information, as well as information related to the quantity, technical configuration, type, destination, and amount of use of service or products subscribed to by a customer of a

[26] Ibid.

regulated utility that is available to the utility solely by virtue of the customer-utility relationship.[27]

Q. Are there any State commissions that have provided specific privacy protection guidance or rules specific to smart grid technologies?

According to the NRRI report referenced earlier, as of 2016, there were seventeen States and the District of Columbia with commission rules in place regarding data privacy including:

1. California	10. Nevada
2. Colorado	11. New York
3. Connecticut	12. Ohio
4. Delaware	13. Oklahoma
5. District of Columba	14. Oregon
6. Iowa	15. Pennsylvania
7. Maine	16. Texas
8. Michigan	17. Washington
9. Minnesota	18. Wisconsin

OPC is aware of at least two other states that has since enacted Commission rules or explicit policy regarding privacy—Arkansas (Docket No 10-102-U) and New Jersey (NJ. Admin. Code 14:4-7.8). We are also aware that Illinois has specific policy in place regarding data access and aggregation standards related to its "AMI Plan" related to the Infrastructure investment and modernization regulatory reform bill which states:

> The AMI Plan shall secure the privacy of personal information and establish the right of consumers to consent to the disclosure of personal energy information to third parties through electronic, web-based, and other means in accordance with State and federal law and regulations regarding consumer privacy and protection of consumer data. . . .
>
> The AMI Plan shall secure the privacy of the customer's personal information. "Personal information" for this purpose consists of the customer's name, address, telephone number, and other personally identifying information, as well as information

[27] Washington State Legislature. WAC 480-100-153: Disclosure of private information. http://apps.leg.wa.gov/wac/default.aspx?cite=480-100-153

about the customer's electric usage. Electric utilities, their contractors or agents, and any third party who comes into possession of such personal information by virtue of working on Smart Grid technology shall not disclose such personal information to be used in mailing lists or to be used for other commercial purposes not reasonably related to the conduct of the utility's business. Electric utilities shall comply with the consumer privacy requirements of the Personal Information Protection Act. In the event a participating utility receives revenues from the sale of information obtained through Smart Grid technology that is not personal information, the participating utility shall use such revenues to offset the revenue requirement.[28]

V. OPC RECOMMENDATIONS

Q. What is OPC recommending to the Commission?

A. OPC is cognizant that more dialogue is necessary from all stakeholders on this issue. As such, we recommend that the Commission order a rule-making workshop to amend Chapter 13 billing rules to account for the substantive changes in billing and data practices and associated privacy concerns. However, in the intermediate period, appropriate preliminary safeguards and practices should be ordered by the Commission. OPC offers up the following general safeguards and practices as recommended actions for the Commission to order through this rate case.

Consent for Disclosure & Green Button Adoption

Individual personal consumer information such as name, address, account number and energy usage, particularly customer-specific energy usage obtained through "smart meters," must be protected from unauthorized disclosure. The highest-possible privacy setting of such information should be the default.

[28] Illinois General Assembly. Utilities (220 ILCS 5/) Public Utilities Act. http://www.ilga.gov/legislation/ilcs/ilcs4.asp?ActID=1277&ChapterID=23&SeqStart=35800000&SeqEnd=40900000

Consumers should not have to take action in order to protect their privacy. As such, KCPL and GMO must not disclose customer information, particularly customer-identified energy usage data, to any third party or affiliate without the specific affirmative consent of the consumer after receipt of complete information relevant to the disclosure and the intended uses of the information. Both KCPL and GMO, and any third party or affiliate should be required to limit the use of such information for the specific purposes the customer authorized.

OPC recommends that the Commission order KCPL and GMO to adopt the Green Button software tool to enable consumers to easily access and securely download their own household smart meter data (*Download My Data*). The Green Button also securely allows consumers the ability to share their smart meter data (*Connect My Data*) with select third parties delivering new services such as smart thermostats, remote home control systems or rooftop solar. Based on OPC's understanding of the Green Button platform, the software should also minimize the potential for affiliate transaction violations.

The Green Button platform has been endorsed by Edison Electric Institute ("EEI") the US Department of Energy ("DOE"), NIST, and is currently being utilized by utilities that have operational AMI in place such as Exelon, PG&E, SDG&E and Southern California Edison. [29]

Data Modeling Standards

Release of aggregate information should be confined to limited public agencies (e.g., Staff and OPC) or academic institutions.

For residential usage, KCPL and GMO should utilize the "15/15 Rule" as the privacy standard required for release of aggregated data. This privacy standard requires that aggregated data include a minimum of 15 customers with no customer's load exceeding 15 percent of the data set's energy consumption.

[29] Green Button Data. (2018)http://www.greenbuttondata.org/

For non-residential usage, KCPL and GMO should utilize the "4/80 Rule" in which aggregated data need to comprise a minimum of four non-residential customers (within an applicable customer class) and no single customer's load exceeding 80 percent of the data set's energy consumption.

OPC further recommends that data only be retained for no longer than three years.

Annual submission of a Cybersecurity Plan ("CSP") and privacy impact assessments ("PIA")

Within six months of rates of going into effect, KCPL and GMO should be required to hold a meeting with members of the Staff and OPC to solicit feedback and discuss the details necessary to submit a comprehensive annual CSP to the Commission that includes, at a minimum, explicit privacy policies and standards, data breach notification plans, and the results of periodic PIAs on the Company's assets and operations in tandem with agreements between third-party contractors and sub-contractors. Moreover, the utilities should utilize an impartial third party consultant to conduct and review the PIAs with the summary of the results made available to the public. This will help to promote transparency and appropriate compliance.

OPC recommends that the Commission order KCPL and GMO to post privacy policy on its website outlining the aforementioned standards and safeguards in place. Staff and OPC should be notified 60 days before any changes are made to its privacy policies and the general public should be notified at least 30 days before any changes are made to its privacy policies.

Q. Do you have any additional comments regarding consumer data privacy protections?

A. Yes. Strong consumer data privacy protections are essential to maintaining the trust of ratepayers. The consequences of a data breach not only affect the customers whose data may fall into the wrong hands, but may also be costly to smart grid entities and utility shareholders. These entities may incur costs to restore the data, to provide compensation such as free credit monitoring for affected customers, to pay any court-awarded damages, and to repair a diminished reputation and loss of corporate good will. Customers (individuals, groups, companies or institutions) should determine for themselves when, how, and to what extent information about them is communicated to others. OPC's recommendations represent a

reasonable path forward as the Commission navigates the potential inherent threats that accompany a more connected and interdependent smart grid.

OPC reserves the right to amend these recommendations in subsequent testimony based on Company responses to on-going discovery. It is not clear, presently, whether or not specific tariff changes would need to be applied to ensure the safeguard compliances referenced above.

Q. Does this conclude your testimony?

A. Yes.

CASE PARTICPATION OF
GEOFF MARKE, PH.D.

Company Name	Employed Agency	Case Number	Issues
Kansas City Power & Light & KCP&L Greater Missouri Operations Company	Office of Public Counsel (OPC)	ER-2018-0145 ER-2018-0146	**Direct:** Smart Grid Data Privacy Protections
Union Electric Company d/b/a Ameren Missouri	OPC	ET-2018-0063	**Rebuttal:** Green Tariff
Liberty Utilities	OPC	GR-2018-0013	**Surrebuttal:** Decoupling
Empire District Electric Company	OPC	EO-2018-0092	**Rebuttal:** Overview of proposal/ MO PSC regulatory activity / Federal Regulatory Activity / SPP Activity and Modeling / Ancillary Considerations **Surrebuttal** Response to parties **Affidavit** in opposition to the non-unanimous stipulation and agreement
Great Plains Energy Incorporated, Kansas City Power & Light Company, KCP&L Greater Missouri Operations Company, and Westar Energy, Inc.	OPC	EM-2018-0012	**Rebuttal:** Merger Commitments and Conditions / Outstanding Concerns
Missouri American Water	OPC	WR-2017-0285	**Direct:** Future Test Year/ Cost Allocation Manual and Affiliate Transaction Rules for Large Water Utilities / Lead Line Replacement **Direct:** Rate Design / Cost Allocation of Lead Line Replacement **Rebuttal**: Lead Line Replacement / Future Test Year/ Decoupling / Residential Usage / Public-Private Coordination **Rebuttal**: Rate Design **Surrebuttal**: affiliate Transaction Rules / Decoupling / Inclining Block Rates / Future Test Year / Single Tariff Pricing / Lead Line Replacement
Missouri Gas Energy / Laclede Gas Company	OPC	GR-2017-0216 GR-2017-0215	**Rebuttal:** Decoupling / Rate Design / Customer Confidentiality / Line Extension in Unserved and Underserved Areas / Economic

			Development Rider & Special Contracts **Surrebuttal:** Pay for Performance / Alagasco & EnergySouth Savings / Decoupling / Rate Design / Energy Efficiency / Economic Development Rider: Combined Heat & Power
Indian Hills Utility	OPC	WR-2017-0259	**Direct:** Rate Design
Rule Making	OPC	EW-2018-0078	Comments on cogeneration and net metering
Empire District Electric Company	OPC	EO-2018-0048	Integrated Resource Planning: Special Contemporary Topics Comments
Kansas City Power & Light	OPC	EO-2018-0046	Integrated Resource Planning: Special Contemporary Topics Comments
KCP&L Greater Missouri Operations Company	OPC	EO-2018-0045	Integrated Resource Planning: Special Contemporary Topics Comments
Missouri American Water	OPC	WU-2017-0296	**Direct:** Lead line replacement pilot program **Rebuttal:** Lead line replacement pilot program **Surrebuttal:** Lead line replacement pilot program
KCP&L Greater Missouri Operations Company	OPC	EO-2017-0230	Comments on Integrated Resource Plan, preferred plan update
Working Case: Emerging Issues in Utility Regulation	OPC	EW-2017-0245	Comments on Emerging Issues in Utility Regulation / Presentation: Inclining Block Rate Design Considerations Presentation: Missouri Integrated Resource Planning: And the search for the "preferred plan."
Rule Making	OPC	EX-2016-0334	Comments on Missouri Energy Efficiency Investment Act Rule Revisions
Great Plains Energy Incorporated, Kansas City Power & Light Company, KCP&L Greater Missouri Operations Company, and Westar Energy, Inc.	OPC	EE-2017-0113 / EM-2017-0226	**Direct**: Employment within Missouri / Independent Third Party Management Audits / Corporate Social Responsibility
Union Electric Company d/b/a Ameren Missouri	OPC	ET-2016-0246	**Rebuttal**: EV Charging Station Policy **Surrebuttal**: EV Charging Station Policy
Kansas City Power & Light		ER-2016-0156	**Direct:** Consumer Disclaimer **Direct:** Response to Commission Directed Questions

			Rebuttal: Customer Experience / Greenwood Solar Facility / Dues and Donations / Electric Vehicle Charging Stations **Rebuttal:** Class Cost of Service / Rate Design **Surrebuttal:** Clean Charge Network / Economic Relief Pilot Program / EEI Dues / EPRI Dues
Union Electric Company d/b/a Ameren Missouri	OPC	ER-2016-0179	**Direct:** Consumer Disclaimer / Transparent Billing Practices / MEEIA Low-Income Exemption **Direct**: Rate Design **Rebuttal:** Low-Income Programs / Advertising / EEI Dues **Rebuttal:** Grid-Access Charge / Inclining Block Rates /Economic Development Riders
KCP&L Greater Missouri Operations Company	OPC	ER-2016-0156	**Direct:** Consumer Disclaimer **Rebuttal:** Regulatory Policy / Customer Experience / Historical & Projected Customer Usage / Rate Design / Low-Income Programs **Surrebuttal:** Rate Design / MEEIA Annualization / Customer Disclaimer / Greenwood Solar Facility / RESRAM / Low-Income Programs
Empire District Electric Company, Empire District Gas Company, Liberty Utilities (Central) Company, Liberty Sub-Corp.	OPC	EM-2016-0213	**Rebuttal:** Response to Merger Impact **Surrebuttal:** Resource Portfolio / Transition Plan
Working Case: Polices to Improve Electric Regulation	OPC	EW-2016-0313	Comments on Performance-Based and Formula Rate Design
Working Case: Electric Vehicle Charging Facilities	OPC	EW-2016-0123	Comments on Policy Considerations of EV stations in rate base
Empire District Electric Company	OPC	ER-2016-0023	**Rebuttal:** Rate Design, Demand-Side Management, Low-Income Weatherization **Surrebuttal:** Demand-Side Management, Low-Income Weatherization, Monthly Bill Average
Missouri American Water	OPC	WR-2015-0301	**Direct:** Consolidated Tariff Pricing / Rate Design Study **Rebuttal:** District Consolidation/Rate Design/Residential Usage/Decoupling **Rebuttal**: Demand-Side Management

			(DSM)/ Supply-Side Management (SSM) **Surrebuttal:** District Consolidation/Decoupling Mechanism/Residential Usage/SSM/DSM/Special Contracts
Working Case: Decoupling Mechanism	OPC	AW-2015-0282	**Memorandum:** Response to Comments
Rule Making	OPC	EW-2015-0105	Missouri Energy Efficiency Investment Act Rule Revisions, Comments
Union Electric Company d/b/a Ameren Missouri	OPC	EO-2015-0084	Triennial Integrated Resource Planning Comments
Union Electric Company d/b/a Ameren Missouri	OPC	EO-2015-0055	**Rebuttal**: Demand-Side Investment Mechanism / MEEIA Cycle II Application **Surrebuttal**: Potential Study / Overearnings / Program Design **Supplemental Direct:** Third-party mediator (Delphi Panel) / Performance Incentive **Supplemental Rebuttal:** Select Differences between Stipulations **Rebuttal:** Pre-Pay Billing
The Empire District Electric Company	OPC	EO-2015-0042	Integrated Resource Planning: Special Contemporary Topics Comments
KCP&L Greater Missouri Operations Company	OPC	EO-2015-0041	Integrated Resource Planning: Special Contemporary Topics Comments
Kansas City Power & Light	OPC	EO-2015-0040	Integrated Resource Planning: Special Contemporary Topics Comments
Union Electric Company d/b/a Ameren Missouri	OPC	EO-2015-0039	Integrated Resource Planning: Special Contemporary Topics Comments
Union Electric Company d/b/a Ameren Missouri	OPC	EO-2015-0029	Ameren MEEIA Cycle I Prudence Review Comments
Kansas City Power & Light	OPC	ER-2014-0370	**Direct** (Revenue Requirement): Solar Rebates **Rebuttal:** Rate Design / Low-Income Weatherization / Solar Rebates **Surrebuttal:** Economic Considerations / Rate Design / Cyber Security Tracker
Rule Making	OPC	EX-2014-0352	Net Metering and Renewable Energy Standard Rule Revisions, Comments
The Empire District Electric Company	OPC	ER-2014-0351	**Rebuttal:** Rate Design/Energy Efficiency and Low-Income Considerations

Rule Making	OPC	AW-2014-0329	Utility Pay Stations and Loan Companies, Rule Drafting, Comments
Union Electric Company d/b/a Ameren Missouri	OPC	ER-2014-0258	**Direct:** Rate Design/Cost of Service Study/Economic Development Rider **Rebuttal:** Rate Design/ Cost of Service/ Low Income Considerations **Surrebuttal:** Rate Design/ Cost-of-Service/ Economic Development Rider
KCP&L Greater Missouri Operations Company	OPC	EO-2014-0189	**Rebuttal:** Sufficiency of Filing **Surrebuttal:** Sufficiency of Filing
KCP&L Greater Missouri Operations Company	OPC	EO-2014-0151	Renewable Energy Standard Rate Adjustment Mechanism (RESRAM) Comments
Liberty Natural Gas	OPC	GR-2014-0152	**Surrebuttal:** Energy Efficiency
Summit Natural Gas	OPC	GR-2014-0086	**Rebuttal:** Energy Efficiency **Surrebuttal:** Energy Efficiency
Union Electric Company d/b/a Ameren Missouri	OPC	ER-2012-0142	**Direct:** PY2013 EM&V results / Rebound Effect **Rebuttal:** PY2013 EM&V results **Surrebuttal:** PY2013 EM&V results **Direct:** Cycle I Performance Incentive **Rebuttal:** Cycle I Performance Incentive
Kansas City Power & Light	Missouri Public Service Commission Staff	EO-2014-0095	**Rebuttal:** MEEIA Cycle I Application testimony adopted
KCP&L Greater Missouri Operations Company	Missouri Division of Energy (DE)	EO-2014-0065	Integrated Resource Planning: Special Contemporary Topics Comments
Kansas City Power & Light	DE	EO-2014-0064	Integrated Resource Planning: Special Contemporary Topics Comments
The Empire District Electric Company	DE	EO-2014-0063	Integrated Resource Planning: Special Contemporary Topics Comments
Union Electric Company d/b/a Ameren Missouri	DE	EO-2014-0062	Integrated Resource Planning: Special Contemporary Topics Comments
The Empire District Electric Company	DE	EO-2013-0547	Triennial Integrated Resource Planning Comments
Working Case: State-Wide Advisory Collaborative	OPC	EW-2013-0519	Presentation: Does Better Information Lead to Better Choices? Evidence from Energy-Efficiency Labels
Independence-Missouri	OPC	Indy Energy Forum 2014	Presentation: Energy Efficiency
Independence-Missouri	OPC	Indy Energy Forum2015	Presentation: Rate Design

NARUC – 2017 Winter	OPC	Committee on Consumer Affairs	NARUC – 2017 Winter Presentation: PAYS Tariff On-Bill Financing
NASUCA – 2017 Summer	OPC	Committee on Water Regulation	NASUCA – 2017 Summer Presentation: Regulatory Issues Related to Lead-Line Replacement of Water Systems
NASUCA – 2017 winter	OPC	Committee on Utility Accounting	NASUCA – 2017 Winter Presentation: Lead Line Replacement Accounting and Cost Allocation

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on July 12, 2012

COMMISSIONERS PRESENT:

Garry A. Brown, Chairman
Patricia L. Acampora
Maureen F. Harris
James L. Larocca
Gregg C. Sayre

CASE: 12-M-0282 – In the Matter of Staff's Review of a New York State Electric & Gas Corporation/Rochester Gas and Electric Corporation Security Breach.

ORDER DIRECTING A REPORT ON IMPLEMENTATION OF RECOMMENDATIONS

(Issued and Effective July 18, 2012)

BY THE COMMISSION:

BACKGROUND

In January 2012, New York State Electric & Gas Corporation (NYSEG) and Rochester Gas and Electric Corporation (RG&E) advised the Department that unauthorized parties had obtained access to confidential information of their customers, including Social Security Numbers, dates of birth, and in some cases, financial institution account information. The Department immediately commenced a review of actions taken by NYSEG/RG&E to inform and assist their customers, including efforts to provide accurate information about the potential impact of this security breach and to provide tools to assist customers in identifying instances in which their confidential information was misused. The Department also immediately began an investigation to identify deficiencies in NYSEG/RG&E systems and procedures regarding the protection of confidential customer information, including those that may have contributed to the incident, and to develop recommendations for corrective action.

The attached Staff Report provides a summary of the Department's oversight of the Companies' response to the security breach, as well as an overview of the Department's investigation of the event. Based on the information in the Staff Report, we direct the Companies to report within 60 days of this Order on their progress in implementing Staff's recommendations and include in such report a response to the concerns raised by the Department as to the Companies' plans with regard to the treatment of costs incurred by the Companies including, specifically, their plans on how to treat such costs in NYSEG's and RG&E's 2012 earnings sharing filings.

DISCUSSION AND CONCLUSION

The attached Staff Report details the events that culminated in a January 2012 communication from NYSEG/RG&E to the Department that a compromise of confidential customer information had occurred as a result of unauthorized sharing of that information on the part of a company contractor. After being so informed, the Department began its oversight of the responses of NYSEG and RG&E to address the security breach and its impact on their respective customers, as well as an investigation of the NYSEG/RG&E event.

The Report makes the following conclusions: (1) there is no evidence to date that any confidential customer information was misused; (2) after the Companies became aware of the security breach, NYSEG/RG&E generally took reasonable actions to inform their customers of the potential impact of the breach; (3) several deficiencies in the Companies' systems and practices contributed to allowing the security breach to occur; (4) NYSEG/RG&E have taken sufficient steps to prevent a recurrence of a security breach similar to that which was announced in January 2012; and (5) NYSEG/RG&E are planning a major revamp of their information systems and data protection security.

We do appreciate the Report's conclusions, although we remain concerned that all aspects of this event be addressed by NYSEG/RG&E. While the immediate steps taken by both the Companies seem reasonable, we want to insure that the Companies

follow through to minimize any potential harm to their customers to the maximum extent practicable, especially because the absence of evidence of any immediate harm does not necessarily indicate that no future harm will occur.

The Report indicates that there exist established and well-recognized best practices for the collection and handling of personally identifiable information (PII). Staff referred to these best practices as a guide to determine the scope of its investigation. Staff concludes its findings by making five recommendations for the Companies to better protect their customers' information and facilitate communication with the Department in the event of any future compromise.

In summary, the Report's five recommendations are that NYSEG/RG&E should: (1) Further refine their policies, processes and procedures regarding confidentiality safeguards; (2) Minimize access to the most sensitive PII by maintaining a strictly "need to know" standard for contractors and employees alike; (3) Conduct, at least annually, an incident response exercise simulating a breach of PII data; (4) Establish company protocols for notification of the Department of Public Service in the event of any significant cyber incident involving a possible compromise of customer data; and (5) Promptly implement steps to better ensure the security of all data stored on company mobile computers and removable data storage media.

We believe it is essential that NYSEG/RG&E consider all opportunities to increase their protection of customer PII. Staff's recommendations provide the Companies with important input so that they may continue to implement corrective measures designed to reduce the possibility of a compromise of data of the kind that occurred in January.

Through this order, we are directing NYSEG/RG&E to file within 60 days a report detailing the measures being taken or to be taken to respond to the above recommendations and a timetable for the implementation of these measures. If NYSEG/RG&E concludes that one or more of the above recommendations should not be implemented or should be modified before implementation, their report should so indicate and should state how the failure to implement the recommendation as proposed

is consistent with best practices for the protection of their customers. If NYSEG/RG&E contend that one or more of these recommendations should not be implemented because of costs, their report should indicate how and to what extent the cost savings from not implementing the recommendation exceeds the benefits to customers from implementation.

In addition to the foregoing recommendations, Staff raises the issue of costs that both the Companies incur in responding to this security breach. We share Staff's concern about its understanding of the manner in which the Companies plan to handle the costs incurred, specifically as those plans relate to including some or all of these costs in the Companies' respective earnings sharing calculation.

We believe that Staff rightly expresses concern that including such costs in earnings sharing calculations could result in a potential recovery from ratepayers of certain of those costs. Staff recommends that we require the Companies to segregate and report all of the costs associated with addressing the security breach, including the customer care costs identified above as well as any incremental investigation and remediation costs, as part of their respective 2012 earnings sharing filings, and that the Commission closely scrutinize any proposal to incorporate these costs in the earnings sharing calculation. In this way, in Staff's view, the Companies should be put on notice that they will be required to justify fully the inclusion of any such expenses in their earnings sharing calculations.

We agree Staff's approach may be necessary and expect NYSEG/RG&E's status report to fully address the Companies' plans regarding the recovery, if any, of these costs, including the specific concerns with their earnings sharing calculations raised in the Staff Report. In their 60-day report, NYSEG/RG&E should also address the Companies' intentions for such cost recovery, and, in particular, whether ratepayers would pay, either directly or indirectly, any portion of these costs and the manner in which such cost recovery is consistent with the Companies' current rate plans.

Moreover, consistent with Staff's work with some other utilities, we are expanding the audit of the systems and procedures in place for the protection of

confidential customer information to New York's other regulated utilities. Such entities are on notice that we expect them to cooperate with the Department's ongoing effort to conduct reviews of their customer data protection measures.

Finally, to the extent that Staff refines its standard and best practices related to protecting PII as a result of such expanded review and audit, NYSEG/RG&E should be aware that Staff may make further recommendations in addition to those contained in the attached Staff report.

The Commission orders:

1. New York State Electric & Gas Corporation/Rochester Gas & Electric Corporation are directed to file a report, as described more fully in the above Discussion and Conclusion, not more than 60 days after the issuance of this Order informing the Commission of their progress in implementing the Report's recommendations. In such report NYSEG/RG&E should also fully address their plans regarding the costs incurred in investigating and addressing this event, including, but not limited to, addressing the specific concerns with their earnings sharing calculations raised in the Staff Report. Moreover, NYSEG/RG&E should explain how their respective approaches are in conformity with the requirements of earnings sharing with their respective rate plans.

2. This proceeding is continued.

By the Commission,

Jaclyn A. Brilling
Digitally Signed by Secretary
New York Public Service Commission

(SIGNED) JACLYN A. BRILLING
Secretary

STATE OF NEW YORK
DEPARTMENT OF PUBLIC SERVICE

New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation Customer Information Security Breach
Case 12-M-0282

Staff Report

July 2012

Schedule GM-2
6/19

SUMMARY

In January 2012, New York State Electric & Gas Corporation (NYSEG) and Rochester Gas and Electric Corporation (RG&E) advised the Department that unauthorized parties had obtained access to confidential information of their customers, including Social Security Numbers, dates of birth, and in some cases, financial institution account information. The Department immediately commenced a review of actions taken by NYSEG/RG&E to inform and assist their customers, including Company efforts to provide accurate information about the potential impact of this security breach and to provide tools to assist customers in identifying instances in which their confidential information was misused. The Department also immediately began an investigation to identify deficiencies in NYSEG/RG&E systems and procedures regarding protection of confidential customer information including those that may have contributed to the incident, and to develop recommendations for corrective action.

This Report provides a summary of the Department's oversight of the Companies' response to that security breach as well as an overview of the Department's investigation of the event. The major conclusions are: (1) there is no evidence to date that any confidential customer information was misused or that the individuals who had unauthorized access to that data had malicious intent; (2) after the Companies became aware of the security breach, NYSEG/RG&E generally took reasonable actions to inform their customers of the potential impact of the breach, and to provide customers with free services to help identify instances in which customer information was misused; (3) several serious deficiencies in NYSEG's and RG&E's systems and practices contributed to the security breach, including the absence of formal procedures applicable to contractors regarding protection of confidential customer information, inadequate limitations on subcontracting by a contractor, and the absence of requirements that systems development and testing be conducted using encrypted or fictitious data; (4) NYSEG/RG&E have taken sufficient steps to prevent a recurrence of a security breach similar to that which was announced in January 2012, and continue to implement Staff's recommendations; and (5) NYSEG/RG&E are planning a major revamp of their information systems and data protection security, for which they expect to issue an RFP

by July 1, 2012, award a bid in the third quarter of 2012 and complete work by the end of 2013.

The Department will continue to review and assess NYSEG's and RG&E's progress in implementing Staff's recommendations and completing their overhaul of their information systems and data protection security, and will report any concerns to the Commission. While NYSEG and RG&E have committed they will not seek recovery of the costs associated with this remedying breach, they will include the costs in their earnings sharing mechanism which could potentially reduce customer's share of future excess earnings. Accordingly, we also recommend that NYSEG and RG&E be required to report the costs associated with this breach and justify their inclusion in any earnings sharing calculations.

BACKGROUND

On or about January 9, 2012, NYSEG and RG&E concluded that there had been unauthorized access to their computer systems containing confidential customer information. On January 23, 2012, NYSEG and RG&E advised the Department that a compromise of confidential customer information had occurred as a result of unauthorized sharing of that information on the part of a third-partycontractor. The Companies' Information Technology (IT) staff had noticed unusual and suspicious network traffic that appeared to be from sources using the contractor's access credentials. NYSEG and RG&E immediately conferred with the contractor and required that the contractor surrender its company access codes.

NYSEG and RG&E further advised that Verizon Business had been retained to conduct an investigation into the cause of the compromise, identify its source, collect evidence, and identify what, if any, broader exposure of sensitive data may have occurred.

Verizon Business found that the contractor had been subcontracting out some of the work it was to perform for NYSEG and RG&E. The contractor gave NYSEG and RGE's access credentials to several persons working for the contractor who were located outside

the United States and accessing NYSEG and RG&E systems from there. Verizon identified the factors that allowed the contractor to give access to others unauthorized to have such access, and how they were able to gain entry to company databases.

Verizon Business did not find any evidence of wrongful intent on the part of the contractor or its subcontractors. There has been no indication to date that the compromised data has been used for malicious or fraudulent purposes.

Following a subsequent briefing by NYSEG and RG&E to Department senior staff, and a sharing of the Verizon Business report, it was determined that the Office of Electric, Gas and Water's Utility Security Section should conduct a review of the full range of NYSEG and RG&E's information systems policies, procedures and technologies that affect or potentially affect the safeguarding of customer data. This review was intended to determine whether any of the cyber security deficiencies that contributed to the compromise in question had been remedied. Further, the review would analyze whether the information system structure of the Companies was sufficiently protected, so as to minimize the possibility of any unauthorized access to sensitive customer information, both from within and outside the Companies.

NYSEG/RG&E ACTION TO INFORM AND PROTECT CUSTOMERS

On January 23, 2012, NYSEG/RG&E began to notify customers of the incident. The Companies mailed more than 1.8 million notification letters to NYSEG and RG&E's residential, commercial and industrial customers to provide information about the breach, how customers may be affected, and the actions that customers should take to determine if their confidential information has been misused. The Companies' also announced that they were offering NYSEG and RG&E customers the option of one year of credit monitoring service from Experian, one of the nation's largest credit reporting entities, at no charge. That service includes a copy of the customer's credit report, a daily monitoring service that provides alerts regarding suspicious activity, and an insurance policy to help cover certain costs in the event that identity theft occurs. The Companies

also augmented its call centers to address an expected increase in call volumes, issued press releases, and provided relevant information on the home pages of its websites.

Shortly after public announcement of the security breach, the Department recognized that the free services that NYSEG/RG&E offered through Experian were provided for residential customers only, and requested that the Companies provide comparable services to non-residential customers. The utilities promptly agreed to do so. Approximately 420 non-residential customers have signed up for those free services.

Staff closely monitored the Companies' activities and customer concerns. We requested and received weekly reports regarding customer inquiries made to the Companies and Experian. More than 65,000 customers have contacted NYSEG/RG&E and more than 600,000 customers have contacted Experian about this issue.

The Department also requested and received weekly reports regarding the number of NYSEG/RG&E customers who enrolled in the free credit monitoring service. Approximately 160,000 residential customers have enrolled in the free credit monitoring service. NYSEG/RG&E had planned to end the ability of customers to enroll in the free credit reporting service as of the end of April 2012. In response to the Department's request, the Companies extended free enrollment in the Experian services through mid-July 2012.

Staff also received reports from Experian regarding the number of new fraud cases that Experian opened for NYSEG/RG&E customers and the disposition of such cases. Experian opens a case when the customer identifies activity regarding his/her accounts that the customer cannot readily explain. Cases are closed when the issue causing the opening has been resolved to the satisfaction of the customer. Through May 31, Experian opened 297 fraud cases for NYSEG/RG&E customers and has closed them all. NYSEG/RG&E reports that they have no information that indicates that there has been any inappropriate use of customer data attributable to this incident.

COSTS INCURRED BY NYSEG/RG&E AND ASSOCIATED RATEMAKING

NYSEG/RG&E reported that they have incurred $3.99 million of incremental costs (through April 2012) to implement the programs described above in order to respond to their customers' situation. According to NYSEG/RG&E, the majority of these costs ($3.2 million) were incurred for customer account monitoring activities. NYSEG/RG&E report that of the customer accounts it monitored, 69% were NYSEG's customers and 31% were RG&E customers, thus it plans to allocate the majority of costs to NYSEG. In its June 22, 2012 response to Staff questions, the Companies indicate that they "will record costs incurred as operating expenses" and "will not be requesting any separate reimbursement or deferral of such costs for future recovery from customers." However, the Companies also state that they will "include such costs in each Company's respective earnings sharing calculation."

Since these costs have been charged to operating expenses, they will reduce the Companies' profits during 2012. Under the terms of the Companies 2010 Rate Order,[1] earnings in excess of a 10.6% return on equity (ROE) are shared equally[2] between customers and shareholders. Since the Companies indicate that they will include such costs in their respective earnings sharing calculations, this may result in a potential recovery of up to 50% (or more) of such costs should the Companies have shared earnings in the rate year ending December 31, 2012. [3]

Given that the Companies intend to include costs attributable to the security breach in their respective earnings sharing calculations, we recommend that the Commission

---

[1] See Cases 09-E-0715 et al., Rochester Gas and Electric Corporation, Order Establishing Rate Plan (issued and effective September 21, 2010).

[2] For 2012, earnings above 11.35% are shared 85% with customers and 15% is retained by the Companies.

[3] For the first rate year 2011, RG&E's electric department reported a return on equity of 10.74% which exceeded its 2011 ROE target of 10.3% by 44 basis points and produced shared earnings of $1.6 million (unaudited). The other operations were between $3 million and $16 million (81 and 131 basis points) below the earnings sharing target of 10.3% return on equity. Pursuant to the terms of the JP, the ROE target for earnings sharing increases to 10.6% for 2012.

require the Companies to segregate and report all of the costs associated with rectifying the security breach, including the customer care costs identified above, as well as any incremental investigation and remediation costs, as part of their 2012 earnings sharing filing. Should those costs affect the level of earnings sharing with customers (including bringing excess earnings to beneath the earnings sharing target of 10.6%) staff recommends that the Companies be put on notice that they will be required to justify the inclusion of any such expenses in their earnings sharing calculations.

SCOPE OF THE DEPARTMENT'S INQUIRY REGARDING PROTECTION OF PERSONALLY IDENTIFIABLE CUSTOMER INFORMATION

Established and well-recognized best practices for the Protection of Personally Identifiable Information (PII) were used to establish the scope of the review conducted by the Department's Utility Security Section.

These best practices were drawn from the National Institute of Standards and Technology (NIST), "Guide to Protecting the Confidentiality of Personally Identifiable Information" (2010). Also referenced for this purpose were the rules for the protection of student information required under the federal Family Educational Rights and Privacy Act (FERPA). Many of the requirements for the protection of student privacy under that act are directly pertinent and readily applicable to the protection of business customer privacy, as well.

From the NIST guidelines and the FERPA rules, staff formed a series of questions grouped into eight subject categories listed below. Staff submitted the questions to NYSEG/RG&E with instructions to supply answers along with documentation to support those answers. Staff later conducted an on-site review of the Companies' responses and documents, and interviewed appropriate NYSEG/RG&E officials and employees for verification and clarification as necessary

The eight subject areas of inquiry were:

Corporate Accountability

In this area of review staff sought to identify the nature and extent of those functional units within NYSEG/RG&E specifically charged with responsibility for protecting customer privacy. Further, staff looked for confirmation that the customer privacy responsibility was fully accepted and shared by senior management and executive level company officials. Written policies were reviewed and documents in support of those policies were examined. NYSEG/RG&E officials were interviewed.

Policies, Procedures and Guidelines

This section of the inquiry examined more specific company policies and procedures, supported by documentation, that govern data access, data transfer, data restriction, data retention, deletion and destruction, and other related matters. Also in this section, policies and documentation were reviewed regarding breach response and notification procedures.

Training, Education and Outreach

Here staff examined the programs in place at the Companies for internal and external outreach and communication regarding privacy and information security. Requirements, or the lack thereof, for mandatory training for all employees and vendors/contractors were examined. Staff reviewed the means by which, and the frequency with which, NYSEG/RG&E ethical standards and codes of conduct are communicated to employees and vendors alike.

Credentialing (Background Screening)

Under this section of review, staff examined the regularly required steps taken by NYSEG/RG&E to be sure of the identity and good integrity of employees, prospective employees, and contractors, and to confirm the identity of customers who interface with NYSEG/RG&E using the Companies online services.

Personally Identifiable Information (PII) Confidentiality Safeguards

In this area of review staff looked at how NYSEG and RG&E handle PII in a variety of important ways -- how NYSEG/RG&E categorize PII, collect it, retain it, segregate it, and periodically review their inventory of PII and destroy that which no longer has any practical business usefulness. Additionally, staff review sought to determine that separate and fully segregated data systems, not containing actual customer data, were used for purposes of systems development and testing.

Network Security

This area of review included an examination of all common network security policies, practices and equipment utilization. Database and electronic traffic monitoring, data encryption, firewalls, antivirus software and malware protection, vulnerability scans, independent third-party assessments, patch management programs, password protocol and discipline, and compartmentalization of employee access rights, etc. were among the specific subjects investigated. NYSEG/RG&E staff was interviewed regarding these practices and measures and produced documentation to confirm their responses.

Physical Security

Staff reviewed physical security measures in place and in force at NYSEG/RG&E as they pertain to the protection of private customer data. The elements of examination in this area mostly concern restrictions on personnel, visitor and contractor access to spaces that house Information systems equipment and terminals.

Incident Response for Possible Compromise of Customer Data

This last area of review concerned the identification and adequacy of plans and protocols in place at NYSEG/RG&E to respond promptly and effectively to a known or suspected instance of unauthorized access to customer data. Also, staff examined the extent to which such plans and protocols were tested through exercises and drills.

SUMMARY OF FINDINGS OF THE DEPARTMENT'S SECURITY REVIEW

While inadequacies in any of the subject areas listed above could result in or contribute to a compromise of sensitive information, the shortcomings that allowed the NYSEG/RG&E problem with its contractor to occur were most concentrated in the area of PII Confidentially Safeguards.

1.) As a matter of policy at NYSEG/RG&E, the use and collection of PII is limited to authorized personnel. However, that policy had not been sufficiently formalized in either company documentation or day-to-day practice. Nor had NYSEG/RG&E followed a practice of carefully communicating to all employees and to all contractors the importance of their ethical and legal obligation to protect customer privacy. NYSEG/RG&E have not been sufficiently explicit in communicating with contractors regarding the obligation they have in protecting confidential information. NYSEG/RG&E are presently developing a program with specific implementing procedures for greater compartmentalizing of employee/contractor access to sensitive customer information. These were serious and aberrational deficiencies.

2.) NYSEG/RG&E have not followed a practice of monitoring the total quantity of PII information that it has collected in its databases and periodically identifying such data that should no longer be retained and therefore destroyed. Their failure in this regard provided a larger amount of PII able to be compromised than should have existed when its systems were breached.

3.) In collecting PII in the normal course of business NYSEG/RG&E have not sufficiently sought to segregate such information into "low-impact" or "high-impact" information (such as Social Security numbers). NYSEG/RG&E advised that they are presently investigating options for this kind of segregation and compartmentalization of more sensitive customer information, most subject to abuse as a result of an unauthorized release or theft

4.) NYSEG/RG&E had been insufficiently attentive to the need to use only "dummy data" or other techniques for protecting against exposure to PII when conducting systems development and testing.

5.) NYSEG/RG&E's inventory of portable (laptop) business computers are vulnerable because of certain security deficiencies. The accidental loss or theft of a NYSEG/RG&E portable computer is an ever present possibility. The result can be a serious compromise of sensitive customer and operational data.

CORRECTIVE MEASURES IMPLEMENTED

To preclude the possibility of a compromise of data of the kind that occurred in January, NYSEG/RG&E have tightened and restricted contractor access to customer data.

1.) Corporate owned portable computers are no longer being utilized by contractors.

2.) Contractors may now only log-in remotely through a secure server, negating the possibility of a contractor sharing log-in credentials with others.

3.) File uploads and downloads to any memory device are administratively disabled and no contractors have the ability to change that configuration.

4.) All contractors are now authenticated when accessing the secure server with multiple layers of validation.

5.) Access to the secure server requires encryption.

6.) All sensitive data, including PII, has been removed from company development and testing systems. All contractors have access only to those systems and do not have access to business and operations systems.

Going beyond the specific vulnerabilities revealed by the January incident, NYSEG/RG&E have assembled a working group within the Companies to comprehensively address data privacy issues and solutions.

The Corporate Security Group of Iberdrola, USA has solicited the assistance of systems security consultants and vendors to evaluate ways to improve the use and collection of PII, and the full range of data and systems security needs. It is expected that an RFP will be issued for the new "Iberdrola Information Security Long Term Framework" by July 1, 2012, with a bid to be awarded in the third quarter of 2012. Work on development and implementation of that new framework will begin in late 2012 and be completed by the close of 2013.

RECOMMENDATIONS

NYSEG/RG&E should:

1.) Further refine policies, processes and procedures regarding confidentiality safeguards. It must fully assess all sensitive information stored on company systems to determine how much has been aggregated, and destroy any data that is not required for business purposes. This will help reduce both the risk and impact of unauthorized exposure by any possible means.

2.) Minimize access to the most sensitive PII, such as Social Security numbers, by maintaining a strictly "need to know" standard for contractors and employees alike.

3.) Conduct, at least annually, an incident response exercise simulating a breach of PII data. This would help to measure the adequacy of the involvement of all stakeholders from across NYSEG/RG&E and the sufficiency of existing plans and procedures.

4.) Establish a NYSEG/RG&E protocol for notification of the Department of Public Service in the event of any significant cyber incident involving a possible compromise of customer data. Following determination (under current company policy) by designated executive and legal officers of the Companies that an IT "critical issue" involving PII has occurred, NYSEG/RG&E should notify the Department within 48 hours of such determination.

5.) Promptly implement steps to better ensure the security of all data stored on company mobile computers and removable data storage media.

Staff has provided these recommendations to NYSEG/RG&E. Some recommendations will be implemented in the near term and the remaining recommendations will be incorporated in the "Information Security Long Term Framework" overhaul project (cited above) currently commencing at NYSEG and RG&E. Staff will continue to monitor their implementation by NYSEG/RG&E and report back to the Commission as needed.

WORK WITH OTHER UTILITIES

Following staff's NYSEG/RG&E review, in order to be sure that the privacy of customer data was being properly assured at the other regulated energy utilities, the Department notified each company that we would be conducting reviews of their customer data protection measures. Each company was instructed to respond to the same set of inquiries as was issued to NYSEG/RG&E and to prepare responses in anticipation of an on-site evaluation of those responses and interviews with appropriate company personnel. The review process focused on best practices and included the issues identified in the NYSEG/RG&E review.

Staff has completed on-site reviews of the policies, practices and procedures for the protection of customer PII at Consolidated Edison and Orange and Rockland, National Grid, and National Fuel Gas. Each company fully cooperated in the conduct of these reviews, making available all documentation and personnel as requested. A comparable

review of Central Hudson Gas and Electric is underway and will be completed shortly. No significant vulnerabilities requiring immediate corrective action were discovered.

Findings to date from these reviews indicate that best practices for the protection of customer information are being generally observed. However, areas for improvement have been identified. For example, some document retention and destruction protocols need to be adhered to more diligently and internal controls on personnel access to data need to be stricter in some instances.

Staff will share its recommendations with the utilities. We expect the utilities to implement these recommendations. Should our follow-up review show utilities are not implementing the recommendations we make, we will report back to the Commission as needed.