STATE OF ILLINOIS

ILLINOIS COMMERCE COMMISSION

Illinois Commerce Commission	)	
On Its Own Motion	)	
	)	
Notice of Inquiry Regarding the	)	16-NOI-1
Regulatory Treatment of Cloud-	)	
Based Solutions	)	

INITIAL COMMENTS OF NORTH SHORE GAS COMPANY AND THE PEOPLES GAS LIGHT AND COKE COMPANY

Pursuant to the Illinois Commerce Commission's ("Commission") Notice in the above-captioned proceeding, North Shore Gas Company ("North Shore") and The Peoples Gas Light and Coke Company ("Peoples Gas") (together, "NSG/PGL") submit their Initial Comments.

North Shore is a corporation organized and existing under the laws of the State of Illinois, having its principal office at 200 East Randolph Street, Chicago, Illinois 60601. It is engaged in the business of purchasing, distributing and selling natural gas to approximately 159,000 customers in Cook and Lake Counties, Illinois. North Shore is a public utility within the meaning of the Public Utilities Act (the "Act").

Peoples Gas is a corporation organized and existing under the laws of the State of Illinois, having its principal office at 200 East Randolph Street, Chicago, Illinois 60601. It is engaged in the business of purchasing, distributing and selling natural gas to approximately 830,000 customers in the City of Chicago. Peoples Gas is a public utility within the meaning of the Act.

North Shore and Peoples Gas are each indirect, wholly-owned subsidiaries of WEC Energy Group, Inc. ("WEC Energy"). North Shore and Peoples Gas receive some services from a centralized service company called WEC Business Services LLC ("WBS"). Certain assets, including certain IT assets, are owned by WBS and costs are allocated to North Shore and Peoples Gas pursuant to Commission-approved affiliated interest agreements. North Shore and Peoples Gas are affiliated with public utilities subject to regulation in the States of Michigan, Minnesota, and Wisconsin and some of the utilities are also subject to regulation by the Federal Energy Regulatory Commission. Consequently, in assessing IT and regulatory issues, WEC Energy must be mindful of the requirements in all the jurisdictions in which it is subject to regulation.

Many of the responses that describe NSG/PGL's experience represent WEC Energy's experience and not just that of the Illinois utilities. One significant implication is the regulatory and cost treatment of assets owned by WBS and not a utility. WBS does not have a jurisdictional rate base and allocates costs to companies that use the asset, *i.e.*, for IT systems residing at WBS, the utilities do not include those systems in their rate bases. A second consideration is that Illinois policy on the topics in this Notice may be inconsistent with the policies of WEC Energy's utilities' other regulators.

For the purposes of these Initial Comments, NSG/PGL consider cloud computing those services offered by third party providers that are at the infrastructure or platform layer. In other words, cloud computing means that the user runs its own servers and operating systems normally, but the user would like to instead run those computing resources off-site in another provider's physical environment. An example of a cloud computing service is Amazon Web Services ("AWS"), which provides virtual servers and

data storage to end users on a subscription based model. The user then uses those computing resources to support an application.

Alternatively, software as a service ("SaaS") will refer to those providers of not only the infrastructure and platform layer, but also the application layer to the end user on a subscription based model. Examples of SaaS are Salesforce.com or Gmail. The application runs entirely off premises. NSG/PGL assume in these Initial Comments that the Commission uses the term "cloud" or "cloud-based" solution for SaaS solutions.

NSG/PGL also note that many of their applications that they would use as a SaaS solution are enterprise wide and likely provided by the shared services affiliate, WBS. WBS, in turn, has a multi-jurisdictional perspective on enterprise solutions that takes into consideration the policies of all its operating jurisdictions.

Cloud vs. On-Premises IT Solutions:

A. Cost:

1. **Identify how costs differ between a traditional on-premises IT system and a cloud-based solution, including all relevant costs and timing of costs.**

   i. In the case of a SaaS solution, costs between on-premises and SaaS alternatives tend to be on par with each other. There are fundamental differences in on-demand scalability and maintenance that, in many cases, can favor a SaaS solution; however the potential costs do vary by component category. When evaluating options, costs, regulatory treatment and the customer perspective are considered. While cost treatment will depend on actual scope and circumstance, the following provides general context for cost breakdowns:

Component	On-premises	Cloud/SaaS
Hardware	Upfront purchase if necessary	N/A – infrastructure is on-demand
Software Set-up and First Year Operations	Upfront purchase plus implementation costs	One time set-up fee plus implementation services
Licensing	Upfront purchase	Part of subscription cost
Maintenance	Annual costs	Part of subscription cost
Ongoing Support	Internal/Contract staff costs	Subscription costs
Customization	Discouraged because of increased cost and risk for on-going support, but often required because of regulatory jurisdiction variances	Minimal, if any, customization; cost prohibitive if/when possible

2. **Describe the costs associated with migrating utility data systems to cloud services. What evidence have stakeholders seen of this shift and what are the results? How long would it take to migrate utility data from on-premises IT to a cloud solution? Provide examples of utility services that have migrated from utility-owned systems to cloud services.**

   i. As NSG/PGL stated in the introduction, cloud computing and SaaS are different, as are the costs and experiences with each approach. NSG/PGL's experience with migrating physical on-premises IT systems to third-party virtual environments, like cloud computing or SaaS, is limited as they have not selected third party alternatives except in limited situations, and the data migration required has been minimal. Typically, NSG/PGL would undertake this at a time of a major project when they re-evaluate their business requirements and review alternatives.

NSG/PGL recently looked at several options for Human Resources ("HR") and Supply Chain enterprise resource planning ("ERP") functions. This would be an example of a SaaS option where the third party provider would provide the hardware, storage and software necessary to support the application. NSG/PGL would likely be responsible for the intra-company network system and connectivity to the third-party provider. NSG/PGL are most likely to move toward a SaaS solution in the HR space as the options are cost competitive and the market offers few on-premises options that support the utilities' business requirements. In short, the markets for HR ERP services have moved to a SaaS subscription model over on-premises solutions. Data migration in any case would be required with the installation of a new ERP solution, whether the solution was on-premises or a subscription model. The costs and challenges in both cases are similar. Going forward, NSG/PGL will continue to evaluate SaaS options at the time that they are life-cycling hardware or evaluating new software.

3. Identify costs associated with training employees to use cloud-based solutions and whether those costs differ substantially from costs to train employees to use utility-owned, on-premises systems.

i. Here, the training costs for cloud computing and SaaS are the same, respectively, as their on-premises counterparts. The training cost differences between on-premises and cloud based solutions are minimal. There are generally no additional complexities involved with using a cloud solution; rather, the training is typically tied to new business processes.

4. **Describe whether and how operations and maintenance costs differ between utility-owned, on-premises systems and cloud services.**

    i. NSG/PGL assume that "cloud services" here refers to SaaS alternatives. Generally the operation and maintenance costs do not differ overall. There are ongoing costs in either scenario, but the costs vary slightly in terms of the source (please see table above).

B. <u>Reliability:</u>

1. **Describe whether and how cloud-based solutions improve safety and reliability at a utility.**

    i. Based on NSG/PGL's experience, there is no difference between cloud and non-cloud solutions pertaining to safety. From a reliability perspective, the reliability risks for on-premises and SaaS solutions are similar, but on-premises is in more direct control by the utility and the SaaS solution is subject to contractual commitments and third party practices to enhance reliability.

2. **Proven Cloud Technologies in Regulated Utilities**

    i. **Identify the cloud services that have proven most successful for public utilities. Identify the differences between a public versus a private cloud, and determine whether one is more appropriate for the utility industry.**

        a. NSG/PGL cannot speak to the experiences of other utilities' use of cloud services. However, WEC Energy has had successful experience with virtualization technology including:

            - Server virtualization to optimize computing resources, increase reliability, reduce data center footprint and simplify hardware replacement;

- Storage virtualization to optimize Storage Area Network storage resources, increase reliability and simplify hardware replacement; and
- Desktop virtualization to optimize computing resources and enable remote work force.

Here, the question is answered in the context of cloud computing. Public clouds are generally available to the public over the internet on a pay for usage model. Private clouds are dedicated to a single user. The primary differences between public and private clouds are:

- Infrastructure components used to implement a private cloud are dedicated to the single customer for whom the private cloud is implemented while components used to implement public clouds are shared by multiple customers.
- There are solutions to create a virtual private cloud in a public cloud environment that is isolated to a single user. The resources are configured to operate on a virtual network within the public cloud environment that is isolated to only a single user.

A private cloud solution provides greater ability to control the environment to meet the business needs of the private cloud customer. If it is important to ensure that a company's data is never comingled with anyone else's (*e.g.*, on Storage Area Network arrays, backup systems, *etc*.), then the private cloud model is preferred because of the added security benefits. Likewise, if it is important to establish absolute physical controls over the infrastructure, then the private cloud model is required.

ii. **Identify public utilities that have adopted cloud-based solutions and what effect cloud services have had on the utility's safety and reliability.**

a. NSG/PGL cannot speak to the safety and reliability outcomes of other utilities. Based on the experience of other WEC Energy utilities, WEC Energy has not experienced a measurable difference in safety and reliability between cloud and non-cloud solutions.

iii. **Identify circumstances where the utility and its customers are better served by a combination of utility-owned, on-premises IT systems and cloud services, a "hybrid" model. What approach best maximizes reliability, safety and security for a utility and its customers?**

a. Those services that are available as a commercial offering in the cloud, and which can be subscribed to in a way that meets utility needs without incurring undue risks or costs, should be evaluated. As described above, there are ERP applications that are less utility centric, such as HR applications, that may be reasonable alternative solutions, but these are not customer facing.

3. Identify successful cloud services adopted by non-utility, but highly regulated, companies or industries. Explain any lessons from their experience that can help maximize reliability, safety, and security for a utility and its customers.

i. NSG/PGL cannot speak to the experiences of other regulated industries.

C. <u>Cybersecurity:</u>

1. Cloud Security

i. Describe whether and how utilities will benefit from the cybersecurity practices provided by cloud-based solutions providers versus those associated with on-premises solutions.

a. Since cloud-based solution providers, and this would include both cloud computing and SaaS, can spread the cost of their support

systems across many customers, they may be able to implement practices such as 24x7 security operations and monitoring center and cybersecurity intelligence analysts with economy of scale. Both the costs and benefits of such practices are spread across many customers and all benefit from the outside expertise, broader experience and overall quality of service that can be more expensive for an individual company to procure or staff.

ii. Identify any cybersecurity benefits of using a cloud-based solution versus an on-premises IT system.

a. A cloud-based solution is beneficial from a cybersecurity perspective when information must be equally available to a variety of non-related entities and leveraged holistically. Information or data can be stored in a cloud-based system and access can be granted to all entities without any external entity granting access to their actual internal systems, thereby reducing access risk.

2. New Risks

i. Describe the extent of new risks introduced (if any) when a utility migrates to a cloud-based solution from an existing on-premises system.

a. When a utility migrates from an existing on-premises system to a cloud-based system, it relinquishes control over a variety of things, including:

- physical access and security to the premises;
- control over the data center, including cooling and power and data connectivity;
- physical control of the system;

- who can access the system;
- who can administer the system;
- where data is stored;
- where data is backed up;
- whether there are any redundancy systems, including network connectivity, power and cooling, and whether those redundant systems are active-passive or active-active, whether and when maintenance, patching and upgrades are performed;
- whether any aspect of support of the cloud-based systems is subcontracted to a third party; and
- whether and when notified of events affecting its data.

Additional potential risks with cloud:

- Loss of productivity due to slow or interrupted communications between the utility and the cloud service provider;
- Increased exposure to distributed denial of service ("DDoS") attack since there are now (at least) two attack vectors between the utility and its data/systems which could be targeted; and
- Increased exposure to man-in-the-middle (MitM) attack since there is now an external path between the utility and its data/systems which could be targeted.

3. Incident Response

i. Describe how cloud-based solution providers can respond to cybersecurity threats in contrast to utilities utilizing on-premises systems.

a. To the extent that they are able to spread the associated costs across multiple customers, third party providers could use 24x7x365 security operations center personnel, cybersecurity threat analysts, on-call "flyaway teams", *etc*. to respond to cybersecurity threats. These methods might be out of budget feasibility for the typical utility. Additionally, to the extent that cloud-

based solutions are implemented in virtual environments, it might be easier for a third party solution provider to move systems to a new guest host, apply threat mitigation measures (patches, upgrades, *etc*.) to the original host and move the system back, with little or no interruption in the service. Virtualization technology to enable this may also be out of budget reach of many utilities. However, virtualization needs to be approached with great caution where regulatory requirements (*e.g*., NERC CIP) may preclude its use.[1]

4. Threat Detection

i. Describe whether and how a cloud-based solution can assist a utility in protecting, detecting, and responding to cybersecurity threats and operational vulnerabilities.

a. Some cloud-based solutions, such as spam/malware filtering of incoming email, provide significant benefit to utilities because they can detect and mitigate threats before they ever enter the utility's network. DDoS mitigation is similar in that it is an external cloud-based service that protects a utility's external facing Internet access point(s) by providing a filter for internet traffic to separate legitimate requests from the DDoS traffic, which helps improve recovery timelines. Likewise, if certain event logs are shared in near-real time with an external cloud-based Security Information and Event Management (SIEM) service, the service can monitor what is going

[1] Although NSG/PGL are not subject to NERC electric reliability requirements, their affiliated electric utilities must meet these requirements.

on external to the utility and look for indications that events logged by the utility's systems may be associated with malicious external activity. Obviously, there is some information security risk in sharing such event information with an external party regarding known vulnerabilities, but the benefits of their expertise and assistance often outweigh these risks.

5. Security Framework for Utilities

i. Identify the key elements and value of a security best-practices framework for utilities to address cybersecurity threats.

a. Key elements of a framework:

- Identify assets, risks and potential threats;
- Protect assets against known risks;
- Detect cybersecurity anomalies and events;
- Respond to detected incidents, newly identified threats and risks; and
- Recover from cybersecurity incidents.

The value of a framework is the ability to provide a common taxonomy and mechanism for organizations to describe current and target state cybersecurity postures, identify and prioritize opportunities for improvement, and communicate cybersecurity risk.

ii. **Identify the security best-practices framework you would recommend for Commission adoption and explain why.**

a. The NIST[2] Cybersecurity Framework provides a solid framework. The development of the framework was born out of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. This EO directed NIST to work with stakeholders

[2] National Institute of Standards and Technology.

to develop a voluntary framework - based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. When combined with a Cybersecurity Capability Maturity Model to evaluate status and opportunity along with a prioritization scheme for improvements, such as the Council on CyberSecurity "Top 20" list, the NIST framework and its references have become the industry standard for managing critical infrastructure risk.

6. **Security Framework for Cloud Providers**
   i. **Identify the key elements and value of standardized security requirements for cloud-based solution providers.**
      a. Please see 5.i.a.

   ii. **Identify and explain the security best-practices framework you would recommend the Commission adopt for cloud services. Explain how this framework differs from security best-practices you would recommend for on-premises systems.**
      a. Please see 5.ii.a.

   iii. **Identify the key elements and value of standardized due diligence guidelines for utilities when selecting cloud-based solution providers. Explain how this guidance is different from selecting on-premises solutions.**

      a. The value of following standard due diligence guidelines is having some level of assurance that the utility will select a viable service provider and have a successful experience. This is extremely important when looking outside of the utility's own controlled environment where only it is responsible for success or failure. Key things to review include:
         - Financial stability of the service provider;

- Proven infrastructure;
- Established Customer Base Geographically distributed datacenters;
- Third party validation and accreditation Service Level Agreement terms and execution;
- Security of data;
- Documented, mandated and monitored security program. Cyber drills or exercises;
- Documented, mandated and monitored data privacy program;
- Documented, mandated and monitored advertising/data mining program;
- Documented, mandated and monitored program for handling sensitive information; and
- Leading data management practices.

iv. **Identify the cloud services selection guidelines you would recommend for Commission adoption and explain why.**

a. Please see 6.iii.a.

7. **Best Practices**

i. **Describe how best practices in protecting sensitive utility and customer information differ between cloud-based hosting and on-premises hosting.**

a. In theory, the only difference between how sensitive utility and customer information is protected in third party environments *versus* on-premises IT systems is who does the work and whether it is done under an internal Operating Level Agreement supporting Service Level Agreements or under a binding contract with data protection stipulations and practices.

On-premises requires the actual measures to protect the information to be undertaken by internal staff, whereas a third party

solution would require more checks and validations that practices and expectations are being met under the terms of the contract.

8. **Compliance**
   i. **Describe whether and how cloud based solutions can improve utility compliance, privacy, and data security**

      a. To the extent that a third party service provider can implement better tools and staff more robustly while spreading the cost across multiple customers, those benefits provided by such tools and staff are an improvement over what a utility can do internally if it cannot afford similar resources due to budget constraints or priorities.

9. **What Should Utilities Avoid Putting in the Cloud?**
   a. **Describe the utility functions - including generation, transmission, distribution, metering, consumption, customer data management and customer experience - that should not be placed in the cloud and explain why. Would your answer depend on whether the information was placed in a public versus private cloud?**

      - There are functions and applications within utilities that are highly complex and/or customized, making them cost prohibitive to use a cloud solution. In many cases this complexity and customization result from regulatory jurisdiction variances or outright regulatory rules around security of critical assets. Some examples of applications that fall into this category include the Electric Management System (EMS) or a full scale customer system.
      - SaaS applications can be subject to latency and availability risks because of connectivity, network configuration and

insufficient computing resources the third party allocates to the application. Anything that is time-sensitive (must be available) should not be exposed to the latency, availability and reliability risks associated with public or private cloud-based hosting. For example, if a Supervisory and Data Control Acquisition ("SCADA") operator needs to see an alarm message related to a field event within two seconds of that event occurring, it would not be good to host the SCADA function in a public or private cloud since there is no way to guarantee connectivity or data throughput speed across external connections.

Beyond SCADA, <u>any</u> process that is business critical is at risk in a <u>public</u> cloud. If latency is a problem, then this risk also extends to the private cloud. If helpdesk or call center functionality is critical, then the related tools must be available. All processes related to helpdesk or call center functionality would break down if Internet connectivity between a cloud service provider and the company were to break down. All important business processes should be evaluated for latency risk before sourcing them to a public or private cloud service.

10. **Connectivity**
    i. **Describe how existing utility IT systems that are not currently interconnected can be made to integrate if hosted in the cloud. What**

are the benefits and vulnerabilities introduced by interconnecting various utility IT services

a. Anything that can be interconnected in a public cloud environment can also be interconnected internally. The benefit is that the third party service may have pre-built interfaces that minimize the effort of information and data transfer (assuming that the functions and outcomes are also core functionality). The vulnerabilities are similar to ones noted in previous questions.

Regulatory Barriers:

A. Ratemaking Treatment:

1. **Does current ratemaking practice discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) provided by third party vendors?**

i. NSG/PGL presume that current ratemaking treatment for the implementation of a cloud computing system would be operation and maintenance (O&M) expenses. Installation costs for on-premises solutions (*i.e.*, purchasing or developing IT system functionality that is housed at the company) would typically be capitalized for ratemaking purposes. Current ratemaking treatment is thus more favorable for on-premises solutions and more appropriate in terms of the rate impact to customers.

For customers, the rate impact associated with recovery of capital assets is more even and better matched with the life of the asset. That is, rates reflect a return on and of the asset over its life. By contrast, the proper rate treatment of an expense item is to add the amount to

rates at the level incurred or to be incurred in a test year. Rather than being spread over the asset life, customer rates would reflect the full expense when incurred. For IT assets of the sort that are the subject of this inquiry, asset / capital treatment is sound ratemaking because the resulting rates would better match the recovery with the customers' benefits from the used and useful period of the asset. For the utility, all else being equal, forgoing a return on an asset for recovery of an O&M expense for systems that serve identical purposes discourages the use of cloud computing. As described above, however, NSG/PGL's analysis would also take into account whether the asset is with its service company or with the utility.

2. **Describe any reasonable justification for accounting ratemaking distinction between investing in cloud-based solutions and investing in on-premises solutions.**

   i. Cloud computing or SaaS *versus* on-premises solutions serve the same purpose for the utility. Each approach is a system that is equally used and useful to the utility in supporting utility service to its customers. Therefore, we believe that each should be treated the same for ratemaking purposes. The NOI (at pages 1-2) cited an apt example of different accounting treatment for systems that are substantially identical (purchasing a product from a vendor versus purchasing a cloud computing license from that same vendor).

3. **Describe whether and how utilities are adopting cloud-based solutions despite its accounting treatment.**

NSG/PGL has generally had limited adoption of a cloud-based solutions, but one notable exception is the NSG/PGL ARC GIS application that leverages cloud for form delivery and processing which ultimately is supported by on-premises servers.

However, as discussed above, we anticipate that WBS could soon adopt some cloud based solutions, such as providing HR services to NSG/PGL employees. For IT assets that are owned by WBS and costs allocated to NSG/PGL pursuant to Commission-approved affiliated interest agreements, the Illinois regulatory accounting treatment (capital *versus* O&M) does not affect the decision. However, were an asset to be one that is appropriately owned by the utility, then the regulatory accounting treatment would be a factor. NSG/PGL cannot speak to the adoption rate of cloud services by other utilities or how they made that decision.

B. Identify alternative ratemaking treatments that would render Illinois utilities indifferent in either choosing to deploy cloud-based solutions provided by third party vendors or continuing with on-premises IT systems owned by the utility.

i. **For each alternative identified, identify the costs and benefits of implementing that alternative.**

ii. **For each alternative identified, identify Illinois administrative rules that would need to be revised, and the revisions(s) required, in order to implement that alternative.**

a. NSG/PGL support treating investments in cloud computing solutions as “intangible plant” (account 303). The benefit of this treatment is that it places identical investments (cloud and on-premises solutions) on equal footing. It removes the rate

incentive for an on-premises solution and means that a cost benefit analysis of different computing solutions would be indifferent to the rate implications. Notably, this change would not create an incentive to choose a cloud solution; it would just eliminate the rate bias in favor of an on-premises solution. Consequently, NSG/PGL did not identify any costs of this approach. Like any investment, inclusion in rate base and recovery of a return on and of the investment would be subject to review in rate cases. A Commission order would be sufficient to implement the policy.

b. A tracker / rider mechanism ("rider") providing for recovery of cloud computing investment as a capital cost is another alternative. NSG/PGL do not recommend this approach although it would likely provide for more timely recovery of the investment. The Commission's authority to authorize riders that are not expressly permitted by statute has been challenged on several occasions. While there is ample support from the Illinois Supreme Court that the Commission has broad discretion in this area[3], some Illinois appellate court decisions have narrowly read the scope of the Commission's authority (despite Illinois Supreme Court authority to the contrary). Absent legislation to expressly allow this approach, its value is uncertain. A benefit

[3] *See, e.g.*, The People *ex rel.*, Lisa Madigan v. Illinois Commerce Commission, 25 N.E. 3rd 587 (Ill. 2015).

of this approach is that, like treating the investment as intangible plant, it places cloud computing on an equal footing with on-premises solutions. A potential cost is that it would be subject to court challenges that would be costly in terms of time and money. Another potential cost is that riders are often subject to annual reconciliation review. These reviews can be time-consuming and costly for the utility, the Commission Staff and other participants. The intangible property approach provides for appropriate review for the justness and reasonableness of the investment. With the caveat that a time-consuming court challenge may ensue, a Commission order, and possibly a rulemaking to define the terms of the rider, would be sufficient to implement the policy.

C. Other Barriers:

1. **Identify and explain any other regulatory barriers that discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) that would otherwise be in the best interest of the utility and its customers. For each barrier identified, identify Illinois administrative rules that would need to be revised, and the revision(s) required, to eliminate that barrier.**

    i. NSG/PGL have no additional regulatory barriers to address.

<u>Additional Benefits of Cloud Deployment:</u>

1. **Describe the types of cloud-based technologies available for electric, gas, and water utilities.**

Generally speaking, technology solutions, which are not typically customized by utilities, vary significantly due to state regulation or are used to operate the grid are available in the cloud. The technology of virtualization can deliver higher levels of availability and reliability for those solutions whether private

cloud or on-premises; it is the principle of the technology. From a cost perspective, generally speaking they are on par with each other and perhaps trending to a slightly lower cost than for the on-premises option.

2. **In electric utilities:**
    i. **Identify specific software services not currently deployed in Illinois available to engage customers in distributed generation, distributed storage, demand response, and energy efficiency programs. Are those tools available as on-premises and cloud solutions, or is only one option available?**
        a. N/A

    ii. **Identify specific services not currently deployed in Illinois that could provide customer engagement portals that improve customer engagement, increase customer satisfaction, and help meet regulatory mandates for verified energy savings and demand reduction.**
        a. N/A

3. **In water and gas utilities:**
    i. **Identify the types of software or services not currently deployed in Illinois that could improve customer engagement and increase customer satisfaction.**
        a. To support mobile app and customer self-service:
            - Robust customer preference center;
            - Alerts capabilities;
            - Mobile app/push notifications;
            - Analytics that easily allow the utility to provide customers insights; and
            - Search engine optimization/search engine management services.
        b. Additional customer feedback/recovery services: post call interaction customer surveys, post web interaction customer surveys, and mobile customer feedback tool.

ii. **Identify the types of software or services not currently deployed in Illinois that could detect leaks and inefficiencies, improve conservation, and lower operating costs.**

a. NSG/PGL are not aware of any other cloud based software or services that would improve conservation, leak detection or inefficiencies, which would lower operating costs.

4. **Describe any additional feature benefits to a utility when adopting a cloud-based solution. For example, what are the benefits of cloud software that analyzes consumption patterns, identifies malfunctioning meters, reduces unbilled energy, or engages in predictive maintenance and load forecasting, among other things.**

i. Additional benefits may include the following:

a. Improved availability and reliability;

b. Improved speed to deliver technology solutions;

c. Flexible capacity:

- Pay as you go vs. investing for end-state needs
- Ability to meet periodic peak needs (Major Storm – High Volume Customer Outage Reports (IVR and Web), High Volume Customer Restoration Communications, etc.)

d. Cost competitive total cost of solution;

e. Improved access to specialized talent (Analytics, Meter Data Management, *etc*.); and

f. Improved ability to provide services that may otherwise be cost prohibitive.

WHEREFORE, North Shore Gas Company and The Peoples Gas Light and Coke Company respectfully submit their Initial Comments.

Respectfully submitted,
North Shore Gas Company
The Peoples Gas Light
and Coke Company

By: Molly Mulroy
Name: Molly Mulroy
Title: Vice President
and Chief Information Officer

Dated this 28th day of April, 2016
Chicago, Illinois 60601

Mary Klyasheff
Koby Bailey
WEC Business Services LLC
Legal and Governance Affairs
200 E. Randolph Street
Chicago, Illinois 60601

MPKlyasheff@integrysgroup.com
KABailey@integrysgroup.com

312-240-4470
312-240-4081