STATE OF ILLINOIS

ILLINOIS COMMERCE COMMISSION

Illinois Commerce Commission On Its Own Motion Notice of Inquiry Regarding the Regulatory Treatment of Cloud- Based Solutions	))))))	Docket No. 16-NOI-01

NICOR GAS COMPANY'S INITIAL COMMENTS
TO NOTICE OF INQUIRY

Northern Illinois Gas Company d/b/a Nicor Gas Company ("Nicor Gas"), through its undersigned attorneys, respectfully submits the following Initial Comments ("Initial Comments") in response to certain questions and issues raised in the Illinois Commerce Commission (the "Commission") Notice of Inquiry ("NOI") Regarding the Regulatory Treatment of Cloud-Based Solutions. In providing the following Initial Comments, Nicor Gas has endeavored to respond to the questions and issues addressed to utilities. As a result, Nicor Gas is not responding at this time to those items in the NOI that are more suitably addressed by vendors or other parties.

I. 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.

The costs vary based on the particular solution at issue. Although Nicor Gas has seen a lower upfront cost, which traditionally is associated with development and infrastructure, there could be a higher ongoing maintenance expense when Nicor Gas is purchasing services similar to that of a subscription or utility service.

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.

As an initial matter, Nicor Gas notes that cloud-based solutions must be defined because the associated information regarding costs can vary dramatically based on the implementation format. For purposes of this response, Nicor Gas defines "cloud-based solution" as limited to cloud native, application hosting, and infrastructure hosting.

Cloud native is an application, such as salesforce.com, built with the intention of remaining a cloud-based system without an on-premises option. Costs are subscription based and assume that the cloud-based solution provides the core functionality needed to manage business processes. In the utility space, there are limited vertical specific cloud native solutions. Those that exist are largely emerging companies focused on applications that are value added solutions rather than core operations functions, such as billing, operations, or financials.

Application hosting is an emerging area with traditionally on-premises solutions, such as customer information systems, where a provider will host and manage an application on behalf of a customer with an alternative licensing model. Pricing for application hosting may transition from a license plus maintenance model to a subscription model where, for example, upgrades may be accommodated.

Infrastructure hosting is not a new solution; however, in many cases, it is now marketed as a cloud-based solution. This is a solution in which a company may choose to license software in a more traditional fashion, but then the company chooses to host the solution in an outside data center in lieu of building internal infrastructure. Pricing for infrastructure hosting may range from a scenario in which a company procures all the equipment and only pays a rack fee to

the provider to a scenario in which a company pays a turnkey monthly expense to the provider with no upfront investment.

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.

The necessary training for end user employees is based on the quality of the application and complexity of the business process. As a result, whether or not an application is in the cloud has little bearing on end user training.

While the need for technical training may be significantly reduced with the implementation of cloud-based solutions, this is only due to the fact that the company transitions to being a consumer of a service as compared to internally building and maintaining a solution from start to finish.

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

The operations and maintenance costs will vary based on the company, solution, and market. In the best case scenario with a cloud-based solution, a company may forgo the majority of upgrade, infrastructure, and change management costs for an application. These costs typically are factored into subscription costs and could be a significant savings as compared to an on-premises solution. However, the significant savings would only materialize if there is a significant user base as in the case of a horizontal industry where a single solution can serve a broad market and thereby lower fees based on the expansive customer roster. These benefits are more difficult to realize, and may, in fact, be non-existent, with certain solutions that have a smaller market, require significant customizations, or need to meet certain operational or security standards.

B. Reliability

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

Reliability is really a function of the quality of the vendor that is engaged to provide the service. Ultimately, the promise of the cloud is found in quality information technology ("IT") service providers offering solutions that are best in class. Where this occurs, a utility may leverage services from an expert or experts with more competencies to ensure reliability and security than could be built internally. There seems to be little dispute over this vision, but utilities need to be very discerning over the quality of their service providers and their ability to, at minimum, meet the service levels of their current internal capabilities. Finally, it is important to note that the response to this question will vary depending on the size and sophistication of a company's IT organization.

C. Cybersecurity

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.

In general, the level of cloud security is largely dependent on the quality of the vendor providing the services. Accordingly, it should not be assumed that all cloud solutions will be more secure than an on-premises solution.

More pointedly, utilities may benefit from the cybersecurity practices provided by cloud-based vendors only if the cloud vendor accepts the utility customer's risk-based requirements to protect the utility data. It is Nicor Gas' experience that large cloud vendors are unwilling to modify their service agreements to meet utility-specific security requirements, thereby forcing the utility to accept whichever baseline security measures a particular cloud vendor implements.

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

One possible benefit would be where a cloud vendor invests in and manages security at a level higher than a utility's internal capability. Again, however, this should not be a blanket assumption.

Another possible benefit would be where a cloud vendor accepts liability for all risks associated with the data entrusted to it. This scenario would offload data breach risk from the utility to the cloud vendor and would result in less first-party risk, less internal control requirements, reduced compliance efforts, and reduced insurance requirements for the utility. The overall responsibility for a data breach of customer data will still lie with the utility, but the mechanisms for responding to the breach would be improved and transferred to the cloud vendor if the contract is written to appropriately capture liability and incident response requirements.

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.

New risks for the utility may include lack of control, prioritization by the vendor, implementation of changes for the benefit of other users of the solution as compared to the needs of the utility, data protection, data retention, and the difficulty of migrating to another solution.

There also is a significant risk surrounding compliance with regulations. Many cloud vendors will not certify compliance with mainstream standards like PCI DSS (payment card industry data security standards). Even those cloud vendors that do certify compliance with mainstream standards will not certify to utility industry specific regulations like TSA PSG (Transportation Security Administration Pipeline Security Guidelines), DHS CFATS

(Department of Homeland Security Chemical Facility Anti-Terrorism Standards), or NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection).

Another risk is presented by standardization of risk and best practice controls (*i.e.*, one-size-fits-all). Each utility determines the level of risk it is willing to accept and which risks it needs to mitigate by investing in security controls. As noted above, many of the quality cloud providers are so large that they are unwilling to modify their standard contracts and service agreements to meet utility-specific requirements. As a result, utilities are forced to accept the vendor's default risk posture and mitigating controls. These circumstances lead to a one-size-fits-all environment in which an adversary could exploit a vulnerability across many utilities.

3. Incident Response

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

The concern utilities face with incident response is that the cloud-based vendor will only respond to cybersecurity threats to its own environment. Many large vendors resist and/or refuse contractual language that requires them to report cyber incidents in their environment to their customers. If a cyber event were to occur in the cloud environment, the response would be limited to the terms of the contract, regardless of the damage that actually was incurred by the utility. For example, if a cyber event were to cause $1 million in damage and customer response activities, and the vendor contract was only worth $100,000 per year, the vendor liability would be capped at the value of the contract, not the actual cost to the utility of the incident response.

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.

Because utilities invest in appropriate controls to protect critical infrastructure assets, the maturity of their security programs tends to be much higher than the security programs of non-critical infrastructure companies like cloud vendors. In addition, cloud vendors may not have staff with DHS-sponsored security clearances, access to threat intelligence regarding nation-state threats, or access to threat databases from the FBI, DOE, or DHS.

5. Security Framework for Utilities

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

The key elements of a security best-practices framework for utilities include a common security language, a baseline set of controls, a risk-based structure, and allowance for compensating controls based on the implementing entity's risk posture.

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

Nicor Gas believes that the "NIST Framework for protecting critical infrastructure cybersecurity" should be the minimum standard used to measure all utility security programs. The NIST Framework was designed to be a risk-based framework to build security requirements for any critical infrastructure sector. This framework follows the already accepted NIST 800 series standards, and it aligns with the mature electric sector's C2M2 model (DOE's cybersecurity capability maturity model).

6. Security Framework for Cloud Providers

i. Identify the key elements and value of standardized security requirements for cloud-based solution providers.

The key elements of standardized security for cloud-based vendors include the same factors listed above for utilities and also include allowance for cloud customers to require specific controls based on their own risk mitigation requirements.

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.

Nicor Gas recommends the NIST Framework described above, as well as the Cloud Security Alliance Cloud Controls Matrix ("CSA CCM"). As described by the CSA, the CCM is "designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider."[1]

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.

As with the CSA CCM, standardized due diligence guidelines should provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The guidelines should be based on generally accepted security frameworks, such as ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum, and NERC CIP. In addition, the guidelines should provide structure, detail, and clarity relating to information security that is tailored to the cloud.

[1] https://cloudsecurityalliance.org/group/cloud-controls-matrix/

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

Nicor Gas recommends the NIST Framework, which is the same standard that utilities should be held to, and the CSA CCM, which provides a common framework to evaluate cloud vendors' cybersecurity controls.

7. Best Practices

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

There is no difference in best practices for protecting sensitive utility and customer information between cloud-based hosting and on-premises hosting. Both solutions require adequate security controls to mitigate risks of inappropriately exposing customer data.

The use of a cloud solution adds the complexity of receiving, processing, and storing customer data on a shared platform or infrastructure. Therefore, vulnerabilities and compromises to customer A could lead to compromises of customer B's data.

8. Compliance

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

In order for cloud based solutions to improve a utility's compliance, the cloud vendor must accept responsibility for compliance with all of the regulations that apply to the utility customer's data. If the cloud vendor were to accept this compliance obligation, then less utility resources would be required to manage compliance and the utility would offload significant risks to the cloud vendor.

Security and privacy improvements could be made if the cloud vendor were to accept the utility customer's risk-based requirements to protect its data. It is Nicor Gas' experience that large cloud vendors are unwilling to modify their service agreements to meet utility-specific

security requirements, thereby forcing the utility to accept whichever baseline security measures a particular cloud vendor implements.

9. What Should Utilities Avoid Putting in the Cloud?

i. 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?

While the market with respect to the cloud is evolving, options are currently limited for cloud native solutions in the large utility space that address core operations such as billing, distribution, and field operations. In examining whether any of these core operations could be moved to a cloud-based solution, the analysis should include traditional measures such as capability, flexibility, extensibility, performance, security, and availability.

Using such an analysis, there are certain corporate IT functions like email, document creation, and storage that may be good candidates for the cloud. Critical infrastructure functions, including SCADA ("Supervisory Control and Data Acquisition"), gas control operations, and plant control systems, should never be placed in the cloud. These are the functions that are specifically targeted by advanced nation-state threat actors. They are also subject to industry specific security regulations (TSA PSG, DHS CFATS, and NERC CIP). Placing these functions into a cloud environment creates a one-size-fits-all environment. That cloud environment would have to implement a security program that was equivalent to the most mature and largest utility customer's security program. The cost of such an environment would place that cloud solution out of reach for smaller utility customers.

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?

Connecting utility IT services creates vulnerabilities as not all data has equal value. Interconnecting systems with sensitive customer information with systems that do not have sensitive customer information will result in all systems being held to the same security standard. Imposing a higher security standard where it is not required is not an efficient and cost-effective use of resources. Best practices encourage the segmentation of high-value data from lower value data so that additional controls can be invested to protect the higher value data. It is a challenge to obtain agreement among different utility services on what is high-value data and what systems require additional controls. If the security standard is not implemented properly, then the entire system is only as secure as the weakest link.

II. 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?

As far as Nicor Gas knows, there is no accounting rule specific to cloud-based solutions in Illinois or the Federal Energy Regulatory Commission ("FERC") Uniform System of Accounts. Generally Accepted Accounting Principles (GAAP) have been recently amended to clarify the accounting for costs associated with cloud-based solutions, and the amendments require those costs to be expensed unless specific criteria are met. In the absence of specific accounting rules, Nicor Gas typically follows GAAP to account for cloud-based solutions. This generally results in expensing most of the costs associated with cloud-based solutions as they are

incurred, rather than capitalizing the costs (and including them in rate base, assuming those costs are prudently and reasonably incurred) and amortizing them over the useful life, as would typically be done for on-premises solutions.

Since there are different types of cloud-based solutions and different pricing and payment arrangements associated with those solutions, it is difficult to address each situation. However, in evaluating options for technology solutions, Nicor Gas considers the overall cost and benefit, including its ability to capitalize costs and recover such costs through rates. Uncertainty in capitalization of any costs incurred in conjunction with cloud-based solutions tends to discourage a utility from considering cloud-based solutions, particularly if the similar on-premises solutions provide clarity in the desirable accounting treatment in ratemaking.

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

Due to the different solutions and pricing/payment arrangements currently available, it is difficult to address each situation. Generally speaking, Nicor Gas believes the similar investment in the equivalent solution should be accounted for the same way in ratemaking regardless of whether the solution is an on-premises solution or cloud-based solution. The current accounting focuses on ownership of the solution and timing of incurring costs, among other factors, in determining the proper accounting treatment. It is particularly the ownership aspect that differentiates the current accounting between on-premises solutions and cloud-based solutions. In ratemaking, Nicor Gas believes there is no reasonable justification to differentiate between utility investments that are similar in nature and provide similar cost and benefit to ratepayers solely based on mere ownership. Although the ownership of software and hardware required for on-premises solutions cannot be ignored, one could argue that the right of a utility to

future service and benefit through cloud-based solutions should also be viewed as a utility's ownership, albeit such ownership would be of an intangible right rather than a tangible asset.

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

Nicor Gas has not implemented any large scale cloud-based solutions that caused the different accounting treatment from on-premises solutions to be a significant issue. There are numerous reasons for not having adopted any large scale cloud-based solutions, including the lack of available vendors and technology, as well as the reasons addressed in Section I above.

4. 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.

Nicor Gas believes the best alternative ratemaking treatment is to account for the costs incurred for cloud-based solutions similar to the costs incurred for on-premises solutions. Under this alternative, utilities will capitalize such costs in Account 303 (Miscellaneous Intangible Plant) and amortize them over the useful life established by the Commission through a depreciation study. Any amortization of the costs associated with cloud-based solutions capitalized amount in Account 303 will follow the same way the assets in Account 303 are currently amortized (depreciation/amortization rather than operations/maintenance). This is the exact accounting treatment for on-premises solutions that Nicor Gas uses today. Nicor Gas does not expect there to be any significant costs to the utilities to implement this alternative treatment as utilities are generally familiar with, and currently using, this treatment in Account 303 for on-premises solutions. The most significant benefit of this alternative ratemaking treatment is to

provide clarity with respect to inclusion in rate base and recoverability of those costs incurred for cloud-based solutions.

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.

In order to implement the alternative ratemaking treatment described above, Nicor Gas believes that 83 Illinois Administrative Code Part 505 must be revised to clarify that costs incurred for cloud-based solutions may be capitalized in Account 303 (Miscellaneous Intangible Plant).

B. 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.

Nicor Gas has not identified other regulatory barriers at this time; however, due to the evolving nature of cloud-based solutions, additional regulatory barriers to utility deployment of cloud-based solutions may be identified in the future.

III. Conclusion

Northern Illinois Gas Company d/b/a Nicor Gas Company appreciates the opportunity to provide these Initial Comments in response to the Commission's Notice of Inquiry and looks forward to continued dialogue regarding the issues addressed herein.

Dated: April 29, 2016

Respectfully submitted,

NORTHERN ILLINOIS GAS COMPANY
D/B/A NICOR GAS COMPANY

By: /s/ Anne W. Mitchell
One of their attorneys

John E. Rooney
Anne W. Mitchell
ROONEY RIPPIE & RATNASWAMY LLP
350 West Hubbard Street, Suite 600
Chicago, Illinois 60654
(312) 447-2800
john.rooney@r3law.com
anne.mitchell@r3law.com