

STATE OF ILLINOIS
ILLINOIS COMMERCE COMMISSION

Illinois Commerce Commission	:	
On Its Own Motion	:	
	:	16-NOI-01
Notice of Inquiry Regarding the	:	
Regulatory Treatment of Cloud-	:	
Based Solutions	:	

MIDAMERICAN ENERGY COMPANY’S RESPONSE TO NOTICE OF INQUIRY

I. Background

On February 19, 2016, the Illinois Commerce Commission (“Commission”) initiated a Notice of Inquiry (“NOI”) to gather information and opinions on the regulatory treatment for various cloud services, among other issues. The Commission explained it was interested in determining whether utility investment in cloud computing is prudent and whether leveling the playing field between cloud and on-premises solutions would encourage utilities to make the most cost-effective investments.

Specifically, the Commission stated it was interested in: 1) comparing cloud services with on-premises IT systems, looking at respective cost, reliability, and security; 2) examining the regulatory accounting treatment of cloud services and discerning whether there are additional regulatory barriers that hinder the adoption of cloud services; and 3) exploring whether additional benefits would accrue from deployment of cloud-based solutions to utilities, customers, the grid, and the environment.

Accordingly, in response to the Commission’s inquiry, MidAmerican Energy Company (“MidAmerican”) provides the following responses to the Commission’s questions.

II. NOI Questions and Responses

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.**

MidAmerican's response:

The difference in costs between traditional on-premises IT systems and a cloud-based IT system is dependent on how each is implemented by the user. For example, providers offering cloud-based infrastructure-as-a-service generally charge for cloud-based IT systems that are deployed and running. Since the cloud-based IT systems can be ramped up or down as required, the customer should not be charged for what is not running.

On the other hand, on-premise deployments require the business to purchase the maximum capacity required beforehand, in order to make it available when needed. Some flexibility is possible because workloads fluctuate. Addressing the fluctuating workload is a practical advantage of the on-premises IT system.

In comparing the costs and benefits of the two different systems, a business must consider various factors. Specifically, in order to take advantage of cloud-based infrastructure on demand and the savings associated with de-provisioning services that are not in use, a business must allocate management and resources to ensure the benefits of cloud-based solutions are maximized. Unless resources are committed to doing that, cloud computing resources may be running unnecessarily, which results in additional fees. The business may not realize the savings and benefits if it incurs fees for cloud-based systems that are constantly running. Therefore, a cost comparison between monthly cloud service fees and costs for on-premise systems is a valuable analysis.

In the case of Software-as-a-Service, MidAmerican observes that software acquisition may be less expensive in the on-premise solution for companies offering both on-premise solutions and a cloud hosted solution. However, it requires an investment in IT resources to run the software. That total cost may be more than the cloud hosted solution, but the business must also consider security and how the system would integrate with on-premise systems. Often these other factors will lead to a desire to

keep systems on-premise to simplify system design.

- 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.**

MidAmerican's response:

MidAmerican does not have a lot of experience migrating utility data systems to cloud services. However, MidAmerican has used some cloud-based IT systems that were developed using cloud space built for a specific purpose. Cloud providers, in general, charge per gigabyte for storage and may charge more depending on what the customer wants from a redundancy and backup capability standpoint. In developing hybrid approaches between on-premise IT systems and a cloud-based solution, bandwidth has been a consideration in determining what virtual capacity can be handled. In talking to other companies using a cloud-based IT service, MidAmerican understands it is not costly to place data into the cloud, but it is quite costly to remove data from the cloud; e.g., there are significant charges if that data is sent anywhere, such as to on-premise systems. If not planned well, data removal could result in significant charges from the cloud provider.

- 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.**

MidAmerican's response:

MidAmerican has not incurred significant costs associated with employee training related to cloud-based solutions, but MidAmerican does not expect significant costs for training employees to use a cloud-based solution versus training for an on-premise solution. IT employees within different departments may manage IT systems independently so there could be some costs incurred from training regardless of which IT solution is used.

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

MidAmerican's response:

MidAmerican considers cloud-based solutions as operating expenses.

MidAmerican considers an investment for an on-premise solution as a capital cost. This is based on the assumption that a cloud-based solution is typically subscription based and the business does not “own” anything tangible. In the case of an on-premise solution, software and hardware maintenance costs would be considered operating expense.

B. Reliability:

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

MidAmerican’s response:

MidAmerican is not aware of an example where a cloud based solution would significantly improve safety or reliability at a utility. Regulatory requirements may preclude using a safety and reliability cloud-based solution hosted by a public cloud.

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

MidAmerican’s response:

i) The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, elasticity and measured service. These characteristics are the same whether public or private.

The difference between public and private cloud is that a private cloud resides in the company’s data center instead of a third-party provider facility. In terms of the public cloud, the third-party provider may dictate the location to the company. In the case of private cloud, the company bears the costs and responsibility of acquiring and managing the hardware and components that go into it. Servers, storage and network equipment need to be replaced from time to time. Investments and resources need to be

allocated to support those systems.

ii) MidAmerican does not have specific examples on how other public utilities have implemented cloud-based solutions and how that implementation may have impacted safety and reliability.

iii) Circumstances where the customer and utility would be best served may be when the utility can take advantage of a cloud provider offering a service at a lower cost without compromising functionality or security. However, the cloud-based solution must not negatively impact regulatory compliance.

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.

MidAmerican's response:

MidAmerican does not have a specific example to share, but MidAmerican notes that cloud hosted e-mail is often a service that is moved to a public cloud provider.

Issues relating to transparency are important, and as such it is important to recognize the service provider may not use the same security standards as the company. Therefore, a written agreement between the provider and company must contain specific language regarding security requirements (e.g. right to audit, vulnerability scanning, etc.)

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

MidAmerican's response:

i) Utilities may benefit where the practices provided by cloud-based solution providers are more mature than the utilities' own capabilities. Larger providers may benefit from scale economies, talent retention and focus that enable enhanced security capabilities which would otherwise be too expensive for a business to self-fund.

Niche cloud providers that have not (and are unlikely to) achieve scale economies may offer a correspondingly inferior security posture.

ii) As noted in the response to section C.1.i) above, the benefits are dependent upon what the provider offers.

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.**

MidAmerican's response:

The Cloud Security Alliance has conducted extensive research on threats posed by cloud computing. The alliance identified nine critical threats to cloud security (ranked in order of severity):

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

3. Incident Response

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

MidAmerican's response:

Large cloud-based providers may have the resources and expertise to respond to threats while smaller niche providers may have significantly fewer resources.

Utilities are dependent on the cloud provider and their contract provisions for primary incident response. If the cloud provider is not responsive, remedies through the court system could be both time consuming and expensive.

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.

MidAmerican's response:

As noted above, whether cloud-based solutions can assist a utility depends on the maturity and resources of the cloud provider relative to the utility and the agreement between the parties stipulating the standards upon which the agreement is based.

5. Security Framework for Utilities

- i. Identify the key elements and value of a security best-practices framework for utilities to address cybersecurity threats.**
- ii. Identify the security best-practices framework you would recommend for Commission adoption and explain why.**

MidAmerican's response:

- i) Key elements and value of security best-practices are addressed by function as follows:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

The activities in the identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks, enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The protect function supports the ability to limit or contain the impact of a potential cybersecurity event.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The detect function enables timely discovery of cybersecurity events.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- ii) NIST Cybersecurity Framework as recommended by the Department of Energy.

6. Security Framework for Cloud Providers

- i. Identify the key elements and value of standardized security requirements for cloud-based solution providers.**
- 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.**
- 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.**
- iv. Identify the cloud services selection guidelines you would recommend for Commission adoption and explain why.**

MidAmerican's response:

i) Key elements of standardized security requirements for cloud-based solution providers are as follows:

- The security of a service organization's system.
- The availability of a service organization's system.
- The processing integrity of a service organization's system.
- The confidentiality of the information that the service organization's system processes or maintains for user entities.
- The privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities.
- Transparency of the service provider processes and adherence to standards set by the company.

ii) For a security best-practices framework, MidAmerican recommends the Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type 2 audit. MidAmerican also considers certification of ISO 27001 as an additional level of assurance. SOC 2 examinations are designed to provide organizations that outsource the operation, collection, processing, transmission, storage, organization, maintenance and/or disposal of their information to third parties a mechanism for assessing governance and oversight at those service providers.

iii) For key elements and standardized due diligence guidelines, MidAmerican recommends the SOC 2 and ISO 27001 because these requirements are well understood industry standards and compliance is easy to determine. Our experience is that immature cloud providers often lack these third-party security control attestations.

See section C.5.i) above, for additional standards describing a secure

relationship between a company and service provider.

In addition to 3rd party audit, there are a number of cloud specific issues that must be well understood:

- How will identity and authentication be managed?
- Is Federation with corporate identity sources supported?
- Is strong authentication supported?
- What security logging is available?
- What is the process for detecting, mitigating and remediating data breaches?
- Who owns the data?
- Will the data be used for other purposes?
- How is service availability measured?
- Does the client have access to service health monitoring?
- What is the disaster recovery plan?
- How does the service manage patches and upgrades?
- Where are the proposed services physically located?
- Where are support staff physically located?
- What 3rd parties does the service rely on? Are audits in place for these 3rd party vendors?

iv) Cloud services should be selected based on a cost, risk, and benefits analysis similar to on-premise solutions.

7. Best Practices

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

MidAmerican's response:

The best practices are fundamentally the same for cloud-based hosting and on-premises hosting. A comprehensive security framework that addresses the entire spectrum of risks is required in either environment.

See sections C.5.i) and C.6.i) above for additional standards describing a secure relationship between a company and service provider.

8. Compliance

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

MidAmerican's response:

Whether and how cloud-based solutions can improve utility compliance,

privacy, and data security depends on a number of variables, including the maturity of the cloud provider relative to the utility and the architecture of the application.

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?**

MidAmerican's response:

Utility systems related to control systems including Distributed Control Systems, Energy Management Systems, Industrial Control Systems, SCADA, Generation Management Systems, Pipeline HMI Systems ("Utility Systems") are not dependent on outside IT systems.

These Utility Systems have little need to interact with IT systems outside the control of the utility and often have required connections into equipment at a site or facility. The regulatory compliance requirements for the Utility Systems require the utility to be in complete control of the physical property and IT connections at the property and the Utility System. These Utility Systems generally do not benefit from deployment into a private or public cloud.

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?**

MidAmerican's response:

There is no fundamental difference between integration with on-premise and cloud services; both are subject to the same security concerns.

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?

MidAmerican's response:

At this time, MidAmerican has not identified any ratemaking practices that have discouraged the use of cloud-based solutions.

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

MidAmerican's response:

Each decision to invest in either cloud-based solutions or on-premises solutions is generally based on the economic costs and benefits for the particular solution. Commission treatment should not preclude any unique ratemaking treatment on a case by case basis. Generally speaking, in most circumstances the generally accepted accounting principles ("GAAP") would apply to account for the investments. In most cases, the GAAP principles will guide the ratemaking treatment associated with the solution.

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

MidAmerican's response:

At this time, MidAmerican applies the GAAP principles to account for cloud-based solutions.

- 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.**
 - 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.**

MidAmerican's response:

As noted in response to question 1, MidAmerican has not identified any alternative ratemaking treatments necessary at this time.

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.**

MidAmerican's response:

As noted above, MidAmerican has not experienced any regulatory barriers discouraging the deployment of cloud-based solutions.

Additional Benefits of Cloud Deployment:

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

MidAmerican's response:

There are numerous cloud-based technologies available for utility functions. For example, there are various technologies to assist customers manage utility accounts or encourage customers to try energy efficiency measures. As noted above, the decision to invest in cloud-based technologies is generally based on the economic costs and benefits for the particular solution.

- 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?**
- 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.**

MidAmerican's response:

i) MidAmerican has identified VisionDSM from Applied Energy Group as a cloud-based software solution for tracking and calculating energy efficiency participation, energy savings and incentives. VisionDSM has customer portals for online enrollment in energy efficiency programs. MidAmerican has not deployed this solution, but is currently exploring the

software for development.

ii) Please see response to 2.i) above.

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.**
- 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.**

MidAmerican's response:

See response to Question 2, above.

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.

MidAmerican's response:

As noted above, MidAmerican has not deployed many cloud-based technologies to support its electric and natural gas operations.