

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	:	

COMMENTS OF THE JOINT SOFTWARE PROVIDER PARTIES
TO THE CLOUD BASED SOFTWARE NOTICE OF INQUIRY

I. Background

Below, you will find the joint comments of Advanced Energy Economy Institute, Advanced Energy Management Alliance, EnergyHub, EnergySavvy, EnerNOC, Inc, FirstFuel Software, Inc , Opower, Inc., and Oracle. hereafter referred to as the “Joint Software Provider Parties”. These Comments are filed and served pursuant to 2 Ill. Adm. Code 1700 Subpart D. The comments were developed collectively by the Joint Software Provider Parties and should not be attributed to a particular member of the group. Contact information for each party that supports these comments can be found in Section III.

The Joint Software Provider Parties appreciate the opportunity to provide the Illinois Commerce Commission (“Commission”) with feedback on these very important issues. The Joint Software Provider Parties are leading providers of cloud-based software services and associations that include members that are cloud-based software service companies. Collectively, these companies provide services for utilities and residential, commercial, industrial, and institutional customers globally. Software

solutions for customers improve utility business operations, maximize the value of demand-side resources, and help engage customers..

II. NOI Questions and Issues

Cloud vs. On-Premises IT Solutions:

A. Cost:

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

The utility industry has gradually and continually increased its use of software over the past several decades, which has yielded significant improvements in utilities' ability to serve customers while providing universal access to affordable and reliable power. Software has served as an enabler to help utilities improve core functions, including more accurately forecasting and planning system build out, more efficiently operating the grid, and more closely engaging with customers by providing a variety of services, from improved billing to marketing for demand-side management services.

Software vendors recognize that the utility industry is becoming increasingly dynamic as new technologies come to market and customer expectations evolve, and there is a need for IT systems being developed today to be flexible, quickly and easily updated, and adaptable for utilities.

Today, software vendors are increasingly transitioning away from on-premise IT systems to cloud-based solutions for many IT functions to continue to create value for utilities and their customers. Cloud-based software is commonly associated with providing increased benefits for utilities and customers, but there can also be cost

advantages for a utility to operate with cloud-based solutions over on-premise IT systems.

The costs of software

In order to access the multitude of benefits from software, some costs must be incurred. Regardless of the function of the software, some of these costs are incurred upfront, such as research and development and implementation, while others are ongoing costs, including upgrades to the software and operations and maintenance. In this discussion, for both on-premise IT systems and cloud-based solutions, these costs can be borne by:

1. **Utilities and their customers.** These costs include procurement, ongoing maintenance, and implementation alongside the vendors. Utilities have had to demonstrate to their regulators that these investments follow rate statutes and are used, useful, and prudent investments.
2. **Software vendors.** These costs include research and development, marketing, and implementation alongside the utilities.
3. **Society.** When benefits are not realized due to either the use of outdated and obsolete software systems or, in some cases, a lack of investment in any software solution, there are real costs that can be attributed to missed opportunities, including reducing grid costs, improving reliability and resiliency of the grid, lowering emissions, and increasing customer engagement and satisfaction.

The cost differences between on-premise IT systems and cloud-based solutions

Traditionally, when a utility purchases an on-premise IT system, there are large upfront setup costs, often including both software and on-site equipment, such as servers, and then dedicated on-site staff who use and maintain the software. These on-site staff spend a majority of their time “keeping the lights on”, running backups and installing patches, but rarely have the capacity to make more significant modifications to upgrade the systems. For an on-premise IT system, the pricing for utilities is typically set up on a *build* and *maintain* basis, where *build* includes all of the upfront costs and *maintain* includes all ongoing costs, which rarely incorporate ongoing additions to the feature set.

Cloud-based solutions require a much lower setup cost, remove the need for most on-site maintenance, and utilize more resources focused on upgrading the software regularly to meet the utility’s evolving needs. All of this is possible because the costs of the software are spread across numerous users (i.e., dozens if not hundreds of utilities are using the same underlying platform). Further, cloud-based solutions offer elasticity, giving utilities the ability to change the capacity of the resources to satisfy their needs. Generally, the costs directly incurred for cloud-based solutions are lower for the utility and higher for the software vendor, but the total costs are lower for cloud-based solutions due to economies of scale and the ability to more efficiently utilize infrastructure. As utilities shift to cloud-based software, they do not view cost as a significant barrier. In a survey of utility executives conducted by Oracle, cost was the

lowest-rated of five concerns.¹In terms of pricing for cloud-based solutions, there are several different models:

- **Subscription-based.** The utility company pays for access, typically, unlimited, or a specific period, either upfront or paid over time
- **Consumption-based.** The utility simply pays for the resources they use such CPU time, network traffic, etc.
- **Market-based.** The pricing is based on supply and demand, where the utility would choose to pay the market price or can bid to use it at a lower price and when the market price reaches that price their workload is activated.

Due to competition between vendors selling to utilities, vendors have had to provide a better value proposition relative to their peer vendors, offer their software at a lower price point, or a combination of the two. Among the Cloud Software Providers in these comments, the most common pricing models are build-and-maintain-based and subscription-based pricing for utilities. More commonly, software vendors use build-and-maintain-based pricing for on-premise solutions and subscription-based pricing for cloud-based solutions, though neither pricing arrangement precludes the ability to include the license of the software.

In an International Data Corporation (“IDC”) survey of ten organizations from a cross section of industries using Amazon Web Services (“AWC”), transitioning to cloud-based solutions has yielded significant value for businesses and their customers by making operations more efficient and cost-effective and providing accelerated solution delivery.² IDC estimated that these AWC customers will capture five-year business

¹ Oracle Utilities, Cloud Technologies are Here for Utilities, Feb 2016.

² IDC, Quantifying the Business Value of Amazon Web Services, May 2015

benefits worth over \$1.5 million per application with a 560% return on investment. These cloud-based services increased business productivity by improving employee performance, reduced downtime as a result of greater stability and reliability, improved IT staff productivity enabling deployment of ~120% more applications per year, and decreased data center-related infrastructure costs.

- 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-premise IT to a cloud solution? Provide examples of utility services that have migrated from utility-owned systems to cloud services.**

Shifting from on-premise IT to cloud-based services is becoming more common, and the efforts associated with making the shift should not be viewed as a barrier to adoption of cloud-based services. Because on-premise and cloud-based systems are often provided by different software vendors, cloud-based providers (such as the companies offering these comments) do not have complete knowledge of how long it takes to “migrate” from one system to another. Rather, we have familiarity with launching our tools in existing utility IT environments. This experience shapes our response to these questions.

There are many factors that determine the costs associated with migration. Some cloud services are entirely new and the utility must decide whether to pursue on-premise or cloud-based, but other services are focused on integrating with and/or replacing existing systems. These latter services - integrating with and/or replacing existing systems - may require significant resources to implement. Examples that can affect the costs of migration include:

- Programming language compatibility (necessary to make sure the systems can communicate with each other)
- Database compatibility (necessary to align data sources across systems, so that customer data is matched with the same customer, for example)
- Third party and other supporting components (necessary to make sure that these components continue to function as intended)
- Graphical user interface (necessary to help users operate the new system efficiently and achieve maximum operational improvements)

Launching a new cloud-based system is similarly fast. For example, one cloud-based provider is able to launch new clients in 15 weeks. This means that a utility could be taking full advantage of a sophisticated software solution in a matter of weeks after signing a contract, compared to months - if not years - to design, build, and implement an on-premise solution.

Because of the affordability and speed of transitioning, utilities are already either in the process of transitioning or are considering switching many of their systems to the cloud. According a recent Oracle survey, large majorities of utilities are planning to shift both legacy and next generation systems to the cloud.³ For legacy systems, this includes customer information systems, mobile workforce management, enterprise resource planning, work and asset management, and outage management. For next generation systems, this includes meter data management, big data applications, business intelligence, and distribution and network automation. In many cases, the transition to the cloud is timed to coincide with the natural lifecycle reinvestment processes for the system as system hardware and software are upgraded. Timing the

³ Oracle Utilities, Cloud Technologies are Here for Utilities, Feb 2016.

migration in this manner avoids the continued higher costs of on-premise systems while being able to now take advantage of the cloud-based solution.

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-premise systems.

Employee training is necessary with the implementation of all new IT systems, either on-premise or cloud-based. There are two reasons why employee training should be cheaper with cloud-based solutions.

First, moving to a cloud-based solution means that utilities need fewer employees on-site for managing the IT tool. This is because the tool is actively managed remotely by the software vendor. Freeing up valuable staff resources allows the utility to align IT services with business and regulatory needs, rather than being locked in to managing on-premise solutions. This creates more opportunities for organizational flexibility.

While the real benefit of freeing up IT resources is to help the utility run more effectively, a secondary benefit is that fewer staff members need to be trained on the new solutions. Simply training fewer employees will reduce training costs significantly. In addition, on-premise solutions, especially those that are custom-built, require highly customized training. Developing these trainings costs money, which will be reflected in what utilities pay the software vendor for the training. For cloud-based software, the training is much more standardized. Many cloud-based software providers have developed off-the-shelf training programs that require minimal customization.

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

The cost differences for operations and maintenance between on-premise solutions and cloud-based solutions can be significant due to economies of scale. The costs are analogous to how utilities operate and maintain power plants. If there were two different scenarios where generators operated 1 GW, where in one case, a hundred different power generators each operate one 10 MW plant, and in the other case, one power generator operates one 1 GW plant, it is likely that the one power generator with one 1 GW power plant will have lower operations and maintenance costs than the hundred different power generators *in aggregate*.

In the context of software, for on-premise solutions, utilities employ talented, IT staff who commonly spend significant time backing up software, applying system patches, and fixing servers and networking equipment. These staff have little time to make significant upgrades to the software.

Cloud-based systems, meanwhile, leverage economies of scale by spreading out the operations and maintenance costs through a much broader base of customers than just one individual utility, resulting in operations and maintenance savings for both utilities and software vendors. IDC has found that customers for cloud-based solutions managed applications ~70% more efficiently compared with maintaining the same environment on-premise.⁴ With cloud-based solutions, IT staff spend less time “keeping the lights on” and can rededicate this time to new projects and innovation. Software vendors, meanwhile, can reinvest these operations and maintenance cost savings to

⁴ IDC, Quantifying the Business Value of Amazon Web Services, May 2015

continually improve products, helping the utility and their customers realize greater benefits and minimizing the societal, missed opportunity costs.

B. Reliability:

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

Modern utilities rely heavily on software along the value chain to provide safe and reliable power, from generation monitoring systems to outage reporting at customer sites. In turn, the reliability and resilience of that software is critical to safe and reliable power delivery.

Cloud-based solutions delivered from trusted cloud providers, such as Amazon and Microsoft, achieve high reliability rates. To give one example: according to cloud monitoring service CloudHarmony, Google Cloud Platform's storage service experienced 14 minutes of downtime in all of 2014⁵. Across the year, that's a 99.9996 uptime percentage.

These high uptime numbers are due to a number of reasons, of which specialization is at the forefront. Amazon Web Services (AWS), a leading Infrastructure-as-a-Service (IaaS) provider, is on course to be a \$10 billion revenue business by the end of 2016⁶. This scale allows AWS to invest in the factors which contribute to reliability to a degree that no single utility, or even group of utilities, could afford.

⁵ Reported by Network World, January 12 2015. <http://www.networkworld.com/article/2866950/cloud-computing/which-cloud-providers-had-the-best-uptime-last-year.html>

⁶ Reported by Computer Weekly, January 29 2016. <http://www.computerweekly.com/news/4500272099/AWS-closes-in-on-becoming-10bn-run-rate-business>

Such reliability factors typically include:

- Hosting software in multiple 'availability zones' that are geographically distinct, so no single external event, such as a storm or power cut, will render the cloud service inaccessible.
- Automated load balancing in front of each availability zone, to seamlessly push internet traffic to a new availability zone in the event of outage, without any downtime for end-users.
- Automatically-scaling processing resources that supply more or less computing power as required at any time, so that a period of high demand will not overload the system and send it offline. For example, a utility outage reporting system must be able to ramp up to handle thousands of requests during a storm or other major outage event.
- Automated data backup, allowing rapid and relatively painless recovery in the event of data corruption or loss.

Finally, it is important to note that cloud-based solutions are not the right answer for every business process. There are some stable processes running reliably through on-premise hardware, and the consideration of whether to move such processes to the cloud should be made on a case-by-case basis.

2. 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.

Utility take-up of cloud solutions has been relatively limited, and delayed,

compared to similar sectors, so there is a limited pool from which to judge the most successful applications. Early utility adopters have typically focused on certain back-end functions, such as HR software for utility employees⁷. Looking internationally, there has been a strong take-up of cloud-based Customer Relationship Management (CRM) tools, such as Salesforce CRM and Microsoft Dynamics. Particularly in competitive energy markets, suppliers and utilities are moving their customer-facing solutions to cloud-based solutions as a way to attract and retain customers through increasing fast-paced commercial innovations.

Under traditional commercial cloud computing arrangements (the ‘public’ cloud), data can be stored and analyzed on servers that are shared by multiple clients. Alternatively, data can be maintained in a private cloud, where hardware and maintenance is provisioned for a single client deployment and data are islanded from other clients’ servers.

The private cloud may provide an additional level of security that is attractive for particularly sensitive data. For example, the Department of Defense’s 2012 cloud strategy document notes that “The Department will not use [shared] commercial cloud services when the loss of information confidentiality, integrity or availability could be expected to have a severe or catastrophically adverse effect on organizational operations, organizational assets or individuals.”⁸

If a utility wishes to store sensitive information in the cloud, it may create similar criteria that trigger what kinds of information can be stored remotely, what kinds must be secured via a virtual private cloud arrangement, and what data may never go to the

⁷ ‘Utility CIO Roundtable’, Electric Light & Power, June 16 2014 <http://www.elp.com/articles/print/volume-92/issue-3/sections/t-d-operations/electric-light-power-exclusive-utility-cios-talk-cybersecurity-cloud-computing.html>

⁸ Department of Defense. Cloud Computing Strategy. July 2012.

cloud.

The recommendation of whether a public or private cloud solution is most appropriate is specific to the organization involved and the service that it is deploying. The utility itself will be in the best position to assess which data require this additional layer of privacy and security, as further discussed under 'Cybersecurity' below.

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.

Cloud solutions have been rapidly adopted in other industries which are highly regulated and share many concerns with the utility industry, such as concern for protecting the personally-identifiable information of customers.

For example, data protection is top of mind in the financial sector, for legal, regulatory and reputational reasons. US financial institutions are impacted by a wide range of national regulations that touch on online security and reliability, in terms of auditing (FedRAMP, ITAR), auditing standards (FFIEC, NIST), and cybersecurity (PIPEDA); alongside international requirements such as the Payment Card Industry Data Security Standard (PCI DSS).

In a survey by the Cloud Security Alliance of the financial sector, 32% of responding firms have an established cloud software policy, and a further 61% are developing one⁹. In other words, only 7% of firms are following a 'no-cloud' policy. This is reflected in the digital nature of modern customers: 57% of the financial firms reported that the majority of their customers are 'digitalized' (over 50% of interactions handled by

⁹ 'How Cloud is Being Used in the Financial Sector', Cloud Security Alliance, March 2015.

digital channels).

Other survey findings from the financial sector adoption of the cloud that are illuminating:

- The most popular reason for adoption of cloud solutions was 'flexible infrastructure capacity' (68% of respondents) which has both reliability and cost impacts – keep services online during high demand events, without requiring the high fixed cost of enough on-premise computing power to cover these spikes in demand.
- Software to improve customer interactions, such as Salesforce CRM, were the joint-highest cloud application adopted (46% of respondents).
- Most financial institutions with an existing cloud strategy (61% of respondents) are deploying a mixture of public and private cloud solutions.

To give a specific financial sector example: Goldman Sachs, a multinational bank that finished 2015 with \$860 billion in assets, has gone from essentially no cloud deployments in 2009 to running around 85% of its 2015 workload in the cloud¹⁰. This scale-up has been driven by the cost, flexibility and reliability benefits of cloud solutions. One of Goldman Sachs' lessons for utilities has been the deployment of both public and private clouds for workloads with different security sensitivities.

Another sector with a firm understanding of the value of security and privacy, healthcare, has seen a similar ramp of cloud software usage. In a survey by the Health Information and Management Systems Society, 83% of healthcare IT executives

¹⁰ Reported by Network World, December 9 2015. <http://www.networkworld.com/article/3013474/cloud-computing/how-goldman-sachs-and-bank-of-america-use-the-cloud-and-containers.html>

reported using cloud services in 2014¹¹. Similarly to financial firms, the two top drivers for cloud adoption amongst healthcare firms were flexible capacity (i.e. gaining access to more computing resources during periods of high demand) and lower costs compared to on-premise solutions.

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.**

Cloud-based computing arrangements create cybersecurity benefits for utilities and their customers. Cloud computing offers scale, distribution, redundancy, and threat suppression capabilities that would be very difficult to match with an on-premise IT deployment. Although there are instances in which on-premise computing is preferable to cloud computing in the utility context—and utilities themselves are best equipped to make that determination—cybersecurity benefits are one of the primary drivers of the rapid adoption of cloud-based solutions in the financial, retail, and healthcare sectors, as well as within the federal government. For example, in 2010, the U.S. Office of Management and Budget (OMB) adopted a “Cloud First” policy that required that federal agencies—including the Department of Energy and the Department of Defense, among others—to “default to cloud-based solutions whenever a secure, reliable, cost-effective

¹¹ ‘2014 HIMSS Analytics Cloud Survey’, as reported by Forbes, July 17 2014
<http://www.forbes.com/sites/louiscolombus/2014/07/17/83-of-healthcare-organizations-are-using-cloud-based-apps-today/#2752aa9c6502>

cloud option exists” before considering on-premise arrangements.¹²

Specific cybersecurity benefits of cloud computing include:

- **Continuous monitoring and preparedness.** Cloud providers prepare for the most sophisticated attacks and employ continuous network monitoring to increase their level of readiness.
- **Distributed architecture and resilience to attack.** Cloud providers distribute the risk of downtime and data loss by maintaining multiple physical locations and building in redundant systems for backup and restoration purposes.
- **Incidence response.** Cloud providers have established industry-leading protocols to respond quickly and efficiently to attacks and ensure the best quality of service throughout.
- **“Futureproof” infrastructure.** Unlike on-premises hardware systems that go out of date and require additional investment for updates, cloud software and hardware is constantly updated to the latest specifications.
- **Scalable, flexible security.** Not all utility data requires the same level of security. Cloud providers offer greater flexibility and scalability to select the right level of security for the right data.
- **Minimization of physical and network seams.** By selecting a remote cloud computing provider, utilities reduce the risk of in-person breach at on premises facility and create fewer seams in the network that are vulnerable to attack through data integration and consolidation.

¹² OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010 <https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf>

The electric and gas distribution grid itself presents a useful analogy of the benefits of cloud computing security. Just as the distribution grid socializes the cost of ensuring secure energy supply for millions of customers, cloud computing arrangements socialize the costs of ensuring cybersecurity for a range of cloud-based storage and software clients. When these clients leverage shared cloud computing architecture, they all benefit from a single security patch, just as all utility customers benefit from enhanced reliability on the grid.

Most important, cybersecurity is a core competency of cloud providers. Maintaining security is essential to their business; a breach would threaten their ability to attract and maintain a client base. Utilities have also vastly increased their on-staff expertise in IT security in recent years, despite the fact that IT security remains distinct from utilities' core energy businesses. By combining utilities' expertise in energy infrastructure and cloud providers' expertise in cybersecurity, customers' interests can be best served.

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.**

The transition to cloud computing infrastructure does not eliminate all security risks. Rather, security remains a challenge requiring constant attention and resources. The State of Connecticut Public Utilities Regulatory Authority described this challenge in its 2014 report, *Cybersecurity and Connecticut's Public Utilities*, "Cybersecurity is not an end state or single accomplishment, but rather a process of continuous attention, vigilance and innovation."

Furthermore, in the context of several high-profile data breaches, it warrants mention that many of them were not specifically enabled by cloud computing, but rather by internal attacks or lapses in security or IT maintenance practices:

- *Edward Snowden leaks.* Snowden, a contractor to the National Security Agency, obtained the leaked documents while employed by the federal government and with administrative access privileges to both on-premise and cloud-based servers.
- *Target hack.* Target's remote threat detection system identified the attack. According to *Bloomberg*, the hack proceeded because executives did not respond quickly enough to the incident.¹³
- *Anthem Health breach.* The data accessed by hackers on Anthem's servers were not encrypted.¹⁴
- *JPMorgan Chase hack.* Hackers targeted applications and programs that run locally (i.e. on-premise) on JPMorgan computers. They were not able to obtain more than contact information for customers, and financial information, much of which is stored and processed in the cloud, remained secure.¹⁵
- *Office of Personal Management hack.* OPM's aging computer systems were vulnerable to attack, and the agency had not conducted a sufficient

¹³ Riley, Michael. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It". *Bloomberg*. 2014. <http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data>

¹⁴ Zetter, Kim. "Health Insurer Anthem Is Hacked, Exposing Millions of Patients' Data." *Wired*. 2015. <http://www.wired.com/2015/02/breach-health-insurer-exposes-sensitive-data-millions-patients/>

¹⁵ Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perloth. "JPMorgan Chase Hacking Affects 76 Million Households." *New York Times*. 2014. http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

inventory of equipment that would have enabled timely upgrades. In addition, OPM did not have adequate staff to guard against the hack.¹⁶

These incidents highlight the range of threats that can impact both cloud-based and on-premise computing solutions. Specific potential cybersecurity risks of cloud computing include:

- **Control over data.** Because data reside off-site in a cloud computing arrangement, there may be a perceived loss of control over this information.
- **Security of data at rest and in transit.** Cloud-based computing enables data to be stored and accessed remotely. The current industry best practice recommends data encryption at rest and in transit.
- **Vendor security management.** Cloud computing and software vendors must be held to industry standards on security—and share their best practices with utility for review.
- **Security and privacy risks through integration.** Integration of utility datasets can create combinations of information that together are more powerful and more sensitive than when maintained separately. Data integration must be conducted carefully to avoid any such security or privacy risks.
- **Access management.** Similar to an on premise computing arrangement, access must be controlled with the utmost care in a cloud computing solution.

It is important to note that many of these security risks are not new to the cloud computing model, but instead are already being addressed through current utility IT

¹⁶ Sean Gallagher. “Why the Biggest Government Hack Ever Got Past the Feds.” *Ars Technica*. 2015. <http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/>

deployments. As in any transition, these risks must be first identified so that they can be planned for and addressed with the appropriate care.

3. Incident Response

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

Cybersecurity incidents range widely, from minor, localized disruptions or credential theft, to organized widespread intrusions resulting in critical damage to infrastructure. Other attacks are designed to be covert and to occur undetected. Utilities and their IT providers must be prepared to defend against this range of attacks, and when threatened, respond quickly and appropriately.

As part of their core business, reputable cloud computing firms will have established incident response protocols and have dedicated significant staff resources to cyber intrusion incident response. For example, Amazon Web Services reports, “Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution.”¹⁷ For on-premise deployments, utilities may or may not choose to employ round-the-clock incident response teams.

If a utility selects a cloud service provider to manage incident response on its behalf, the utility will benefit from increased vigilance. Yet, security remains a shared objective. Clear protocols must be established so that vendor staff are empowered to respond to threats while also ensuring that utility staff are appropriately informed and able to authorize important security actions. Ensuring that these protocols are followed will necessarily be a shared responsibility between utilities and their cloud providers.

¹⁷ AWS. Amazon Web Services: Overview of Security Processes. June 2014.
http://awsmedia.s3.amazonaws.com/pdf/aws_security_whitepaper.pdf

A further benefit of cloud-based incident response is minimization of downtime. Cloud applications are routinely deployed in an “N+1 configuration,” such that in the event of a breach or failure at one site, there is enough redundancy in the network to ensure that systems remain operable, with minimal downtime. By contrast, if there is a local interruption at an on-premise computing deployment, the utility will likely have no backup option to engage.

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.**

Threat detection and incident response are highly related in that the single most important aspect of an incident response procedure is the ability to recognize—or even anticipate—an intrusion. Thus, in the same way that cloud computing arrangements improve incident response through continuous monitoring, utilities can also benefit from similar improvements from continuous, automated threat detection in cloud-based solutions.

For on-premise IT deployments, threat detection is often managed on a periodic basis, rather than continually. Staff rely on process logs and periodic reviews to determine security performance over time. The transition to constant monitoring represents a significant improvement in service, one in which automated alerts can be triggered to identify and stop a threat before significant damage occurs. The Department of Defense specifically cited this benefit in its 2012 cloud computing strategy memo, and the DOD has implemented protocols to detect malicious code

signatures across its cloud deployments. Enterprise cloud computing providers maintain similar programs that, when malicious code is detected, can react instantaneously to mitigate the threat.

In addition to the 24/7/365 nature and increasing automation of cloud-based threat detection, cloud computing providers also routinely conduct third party penetration tests that are specifically designed to identify and patch weaknesses in their network architecture. These third-party tests prepare cloud solutions providers to respond more rapidly to future intrusion attempts by malicious actors.

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.**

There are several existing cybersecurity frameworks that outline best practices for utilities in securing and managing energy and customer data. Developed by state, national, and international coalitions, these documents may serve as a guide to utilities and regulators and be localized to the Illinois context, as appropriate.

Current cybersecurity frameworks and best practices guides include:

- The National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity"
- NERC Critical Infrastructure Protection (CIP) Program
- Connecticut Public Utilities Regulatory Authority's "Cybersecurity and Connecticut's Public Utilities" report
- New Jersey Board of Public Utilities Comprehensive Cybersecurity

Requirements for Regulated Utilities

The most recent of these frameworks, New Jersey Board of Public Utilities' cybersecurity framework was adopted on March 18, 2016 and calls for regulated electric, natural gas, and water/wastewater utilities to develop and maintain cybersecurity plans with the following requirements for Cyber Risk Management:

- ***“Identify*** – *Annually inventory critical systems and document changes.*
- ***Analyze*** – *Annually assess and prioritize cyber risks, including physical risks, to identified critical systems [...]*
- ***Control*** – *Implement administrative, technical (logical and physical), and compensating controls, alone or in combination, to mitigate prioritized cyber risks [...]*
- ***Measure and monitor*** – *Annually review risk assessment methodology to identify and incorporate revisions as appropriate.”*¹⁸

NIST describes its cybersecurity framework as “an organizing construct for aligning and communicating requirements” and cautions that it is not designed to create additional regulation. The NIST framework does however propose best practices along similar lines to those outlined by the NJ PBU. Broadly, these include the following categories:

- **Identify** – Conducting an inventory of hardware, software, communication and data flows.
- **Protect** – Managing physical and remote access, training, security of data at rest and in transit, logs and records of access.

¹⁸ New Jersey Board of Public Utilities. *In The Matter Of Utility Cyber Security Program Requirements*. Docket No. A016030196. Agenda Item 6A. March 18 2016.

- **Detect** - Continuous monitoring, detecting anomalies, vulnerability scans.
- **Respond** – Response planning, communications, damage mitigation.
- **Recover** – Restore operations and incorporate lessons learned.

In addition to these frameworks, policymakers should also track the development of the “Cybersecurity National Action Plan” announced by President Obama in February 2016. The National Action Plan will include a Cybersecurity Framework report to be published within the next year.

Beyond those already identified in the frameworks noted here, additional cybersecurity best practices include security monitoring/logging to identify potential threats, ensuring data encryption at rest and in transit, imposing system security, hardware security, and physical access limitation protocols, as well as conducting independent third-party reviews of security practices and penetration test and improving staff level readiness through a governance process and regular staff training sessions. Security best practices should also be regularly reviewed and updated to ensure that utilities and their partners are at the vanguard of cybersecurity practice.

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 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.

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

Vendors should be expected to maintain security practices that are equally rigorous to those followed by utilities; however, cloud and SaaS providers are not subject to the same level of regulation as utilities are. As the regulated entities, utilities are well positioned to serve as the primary vetting agent of vendor security, with the goal of aligning vendor security requirements to the utility's own systems and security practices, as well as any requirements proposed by the Commission. This is common business practice today and should remain so.

In the context of this utility-vendor model, FINRA's 2015 "Report on Cybersecurity Practices" offers a useful example of maintaining security within the financial sector across vendors [emphasis added]:

"Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:

- ***performing pre-contract due diligence on prospective service providers;***
- ***establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access and which govern both the ongoing relationship with the vendor and the vendor's***

- obligations after the relationship ends;*
- **performing ongoing due diligence** on existing vendors;
- **including vendor relationships** and outsourced systems as part of the firm's ongoing risk assessment process;
- **establishing and implementing procedures to terminate vendor access** to firm systems immediately upon contract termination; and
- **establishing, maintaining and monitoring vendor entitlements** so as to align with firm risk appetite and information security standards..."

Whether in the context of an on-premise deployment or in an agreement with a cloud provider, utilities should practice similar due diligence. Security is equally important in both contexts.

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 should be no difference in the protection of sensitive utility and customer information. Whether the information is stored on premise or in the cloud, it should be protected in either case. In practice, there are some distinctions in terms of best practices.

For on-premise deployments, utility and customer data should be stored on servers or client hardware that are frequently updated and patched for security. If not, these data may be at security risk. For example, on-premise client machines may run older versions of operating systems that are no longer supported by the original

manufacturer. Staff may store or download data to these machines that can then be intercepted by malicious actors. In this case, a key goal for the utility will be to ensure that all hardware and software is up-to-date on machines that work with sensitive data. For a cloud computing provider that is constantly updating hardware and software to the best available options and one that manages data storage and analysis in cloud servers, this is less of a concern.

For particularly sensitive information stored in the cloud, a possible best practice is to use a virtual private cloud arrangement. Under traditional commercial cloud computing arrangements, data can be stored and analyzed on servers that are shared by multiple clients. Alternatively, data can be maintained in a private cloud, where hardware and maintenance is provisioned for a single client deployment and data are islanded from other clients' servers. This may provide an additional level of security that is attractive for particularly sensitive data. For example, the Department of Defense's 2012 cloud strategy document notes that "The Department will not use [shared] commercial cloud services when the loss of information confidentiality, integrity or availability could be expected to have a severe or catastrophically adverse effect on organizational operations, organizational assets or individuals."¹⁹

If a utility wishes to store sensitive information in the cloud, it may create similar criteria that trigger what kinds of information can be stored remotely, what kinds must be secured via a virtual private cloud arrangement, and what data may never go to the cloud. Again, the utility itself will be in the best position to assess which data require this additional layer of privacy and security.

¹⁹ Department of Defense. Cloud Computing Strategy. July 2012.

8. Compliance

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

Cloud solutions providers have prioritized compliance with state, federal, industry, and international standards for privacy and security compliance. The key benefit of selecting such a provider is that many of these compliance options are readily deployable “off-the-shelf” as part of a cloud platform, rather than through individualized application-specific customizations that can be costly to implement.

As an illustration of the range of compliance options it serves, Amazon Web Services provides the following table at <http://aws.amazon.com/compliance/>:

 Certifications / Attestations	 Laws, Regulations, and Privacy	 Alignments / Frameworks
DoD SRG	CS Mark [Japan]	CJIS
FedRAMP	DNB [Netherlands]	CLIA
FIPS	EAR	CMS EDGE
IRAP	EU Model Clauses	CMSR
ISO 9001	FERPA	CSA
ISO 27001	GLBA	FDA
ISO 27017	HIPAA	FedRAMP TIC
ISO 27018	HITECH	FISC
MLPS Level 3	IRS 1075	FISMA
MTCS	ITAR	G-Cloud
PCI DSS Level 1	My Number Act [Japan]	GxP (FDA CFR 21 Part 11)
SEC Rule 17-a-4(f)	U.K. DPA - 1988	IT Grundschutz
SOC 1	VPAT / Section 508	MITA 3.0
SOC 2	EU Data Protection Directive	MPAA
SOC 3	Privacy Act [Australia]	NERC
	Privacy Act [New Zealand]	NIST
	PDPA - 2010 [Malaysia]	PHR
	PDPA - 2012 [Singapore]	UK Cyber Essentials

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?**

The determination of which data to store, process, and manage through cloud-based computing arrangements is one best made by the utility itself in accordance with its security and critical infrastructure planning procedures. Not all data are equally sensitive, and the determination of where datasets resides should reflect those various levels of sensitivity.

Some utilities may choose not to store, analyze, and process distribution grid data in the cloud, under the assumption that storing this information remotely could leave the grid open to attack by malicious actors. Again, this is a determination best left to the utility itself, as a range of utility computing needs will require a range of solutions. As Department of Defense Chief Information Officer Terry Halvorsen noted of the DoD's "hybrid" approach to cloud computing, each solution warrants individual consideration as to the level of connectivity and security required:

"We will use a hybrid approach to Cloud that takes advantage of all types of Cloud solutions to get the best combination of mission effectiveness and efficiency. This means in some cases we will use a purely commercial solution, which we have done with Amazon on public facing data, in others we will use a modified private Cloud hosted in commercial solutions."²⁰

Regulated utilities will no doubt require similar considerations for grid-level and customer-specific data storage and maintenance decisions. It also important to note that

²⁰ Defense Information Systems Agency. "Best Practices Guide for Department of Defense Cloud Mission Owners V 1.0" August 2015.

this question does not have a static answer. What a utility may choose to place in the cloud in 2016 may differ significantly by 2018. As more software providers shift to cloud-only options, regulators become more accustomed to cloud solutions, and utilities begin to elect cloud-based solutions on their own, the common “best practice” may shift along with the marketplace itself.

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?**

Although it is an optional component of a utility transition to cloud-based computing, integration of data sets has the potential to be highly valuable to utility operations. Through better interoperability, utilities can achieve operational efficiencies that would previously require additional investment and significant in-house resources. Even so, there may be instances where data integration is unwieldy or overly onerous to implement and therefore should be avoided.

As an illustration of one potential value stream of data integration, Northeast Energy Efficiency Partnerships published an extensive report on “Energy Efficiency as a T&D Resource,” where it encouraged the practice of using targeted energy efficiency to delay or defer investments in the distribution grid (programs also known as “non-wires alternatives” projects).²¹ Traditionally, these projects require significant time and resources for bringing together disparate information sources about utility capital plans,

²¹ Chris Neme & Jim Grevatt, NEEP. “Energy Efficiency as a T&D Resource.” 2015.

distribution plans, demand-side management information, as well as customer and building data. The report notes that this organizational shift can itself be a deterrent to considering non-wires alternatives. However, if such data were fully interoperable and easy to query, these projects would be much easier to scope.

It is important to note that the increased interconnectivity of data does not inherently create vulnerabilities. There may be valid concerns about putting data “online” that has never been internet-addressable in the past, which could potentially create a greater understanding of generation and grid activities by malicious actors. These potential weaknesses can be mitigated by data deidentification, encryption, and other best practices discussed above and should not deter utilities from integrating disparate datasets.

The benefits of better data integration include system efficiencies to reduce line losses and outages, the ability for customers to access relevant energy services programs in their area, and potentially lower costs at the generation, transmission, and distribution levels of the grid. Due to challenges of data integration, many of these benefits have yet to be realized; and therefore, for many cloud computing and SaaS providers, data integration is a key value proposition considered by potential utility clients.

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

The pace of technological change is unprecedented as utilities begin to take advantage of information technologies in new and different ways to improve the overall performance of the utility system, in terms of reliability, cost, and customer engagement. At the same time, the delivery of technology solutions is rapidly shifting from on-premise deployments to cloud-based deployments in order to deliver higher levels of innovation, solution reliability and improved cost effectiveness (as discussed above).

Ratemaking should not discriminate between deployment approaches. . Ratemaking can and should allow a utility to be rewarded for the critical investments that it makes in the systems that are clearly driving improvements in reliability and service for the end consumer. Regardless of the deployment approach, ratemaking should reward the utility for delivering systems in the most effective and reliable manner.

Current ratemaking practice as implemented by the utilities in Illinois differentiates between the two most common ways these IT deployment approaches are accounted for. On-premise deployments often entail a significant up-front expenditure in software, hardware and implementation services, the majority of which the utility can capitalize and add to the capital rate base. The ongoing costs of operating the system

are commonly treated as part of the utilities operating expenses. Cloud-based solutions are often accounted for as service contracts as opposed to capital assets. Generally, service contracts are considered an operating expense. As a result, the choice of a cloud-based deployment implies that the utility forgoes the benefits of a capital asset and the ability to earn on that investment.

As a result, utilities are financially incented towards an on-premise approach, even if it is the more expensive, less reliable, and less innovative option. There are two reasons why utilities may prefer a “capitalized” solution. First, they would like to earn a rate-of-return on the purchase, just like they do with on-premise software. However, many cloud-based software purchases are relatively small (less than \$1 million per year). Purchases this small will not make a material difference to a utility’s ratebase, which is often hundreds of times this size. Thus, the ability to earn a rate-of-return is particularly relevant only for the biggest cloud-based software purchases. Second, and perhaps more important, utilities often have more budget flexibility within capital budgets. This is because any increase in operations spending decreases a utility’s near-term earnings, while utilities are not similarly incentivized to reduce capital spending. This is particularly relevant between rate cases.

Importantly, we think that utilities have assumed that cloud-based software is not a capital expense. This is likely because utilities characterize a cloud-based software purchase as a service contract instead of as a license to use a valuable asset. In fact, there is actually significant ambiguity in the regulatory rules about how to characterize a cloud-based software purchase. The ICC can clarify this ambiguity either through informal guidance or a formal rule change. If the Commission provides this clarity, then

current ratemaking practice can make utilities indifferent between cloud-based and on-premise solutions.

The ICC should provide guidance to utilities that the Commission's expectation is that utilities should make the best investments for their customers, and that the Commission will approve requests to treat cloud-based and on-premise software equally.

There are other ratemaking concepts that should not change. For example, utilities should only be allowed to recover their costs (including a rate-of-return) for prudent investments. The ICC should not make any changes to rules that require that utility investments deliver positive outcomes for customers.

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

Utilities are currently addressing the accounting differences in two primary ways. The first is the utilization of cloud-based systems as part of the delivery of a larger project to build and deliver a capital asset. For example, the use of Primavera project management solutions for the planning and managing of a large capital construction project, such as a generation, transmission, or distribution facility.

The second approach, again part of a larger capital IT investment, is the use of cloud-based infrastructure and platform services to support the development and testing environments that are required during the peak periods of a systems implementation effort being delivered on-premise. Historically the utility would have purchased the hardware and software required to satisfy the highest level of forecast demand for computing resources - unnecessarily increasing the cost of the implementation project

and the ongoing operating expense of the system.

Utilities are also using cloud-based software for programs that have a dedicated budget. For example, many utilities have a dedicated demand-side management budget. When this dedicated budget exists, they are indifferent between solution types and are rapidly embracing 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.**

There are two primary alternatives for consideration, and they range from very simple to complex. We are encouraging the ICC to embrace the simplest path forward. By doing this, the Commission will reduce the need for rule changes (or legislative changes), move toward a solution faster, and work within existing norms for contract structures in the cloud-based software industry.

We believe that the Commission can work within existing regulatory rules to render Illinois utilities indifferent. In Section 415.10 of the Administrative Code, Illinois has adopted the Federal Energy Regulatory Commission's Uniform System of Accounts (FERC's USOA) by reference. The Commission has made minor changes to FERC's USOA, none of which impact the treatment of cloud-based software.

FERC's USOA is silent on accounting treatment for cloud-based software. In fact, FERC is silent on most of the biggest software issues facing utilities today. For example, there is no specific account for customer-information systems, which routinely cost over \$100 million.

It's also very easy to find places where cloud-based software could fit within FERC's USOA. For example, Account 303 "Miscellaneous Intangible Plant" is defined as:

"This account shall include the cost of patent rights, licenses, privileges, and other intangible property necessary or valuable in the conduct of utility operations and not specifically chargeable to any other account."

A license to use a cloud-based software platform clearly fits within this definition. This account rolls into Account 101 "Electric Plant in Service", which means that it is clearly a capital account. Putting cloud-based software in this account is a straightforward way to "capitalize" cloud-based software. The ICC could do two things to encourage utilities to use this approach. First, the Commission could simply tell the utilities (via a letter) that they interpret "other intangible property necessary or valuable in the conduct of utility operations" to include contracts for cloud-based software. Second, the Commission could amend the FERC USOA language to the following:

*"This account shall include the cost of patent rights, licenses, privileges, **contracts for cloud-based software**, and other intangible property necessary or valuable in the conduct of utility operations and not specifically chargeable to any other account."*

This simple amendment would become Section 415.3030 of the administrative code.

The second approach is reconsidering the accounting treatment of cloud-based deployment approaches as a service contract. Recent revisions to GAAP rules²²

²² FASB Update 2015-05 for Intangibles—Goodwill and Other—Internal-Use Software (Subtopic 350-40)

regarding the treatment of fees paid in a Cloud Services Arrangement provide for the capitalization of Cloud services in certain circumstances. Utilities are evaluating this FASB update with their accounting advisors and making decisions as to how it may be interpreted. If the utility and its auditors agree that the rules of capitalization have been met, then the ratemaking process should honor that accounting approach as it has in the past with on-premise IT investments. Again, this does not require any change to regulatory accounting rules.

A. 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.**

If utilities and their technology providers address the questions and concerns addressed in prior sections regarding security and privacy, and ratemaking in Illinois does not discriminate but rather treats on-premise and cloud-based deployment models equally, no other barriers for the adoption of cloud-based solutions should exist. Each utility would be in a position to evaluate various technology alternatives based on the capabilities and cost effectiveness of the varying solutions, and choose accordingly.

III. Contact Information

Contact information for the Joint Software Provider Parties:

J.R. Tolbert
Advanced Energy Economy Institute
1000 Vermont Ave NW, Third Floor
Washington, DC 20009
jtolbert@aee.net

Katherine Hamilton
Advanced Energy Management Alliance
38 North Solutions
Katherine@38northsolutions.com

Laura Kier
Senior Associate, Market Operations
EnergyHub
232 3rd St C201
Brooklyn, NY 11215
kier@energyhub.net

Jake Oster
EnergySavvy
159 South Jackson St, Ste 420
Seattle WA, 98104
Jake@energysavvy.com

Greg Poulos,
Director, Regulatory Affairs
EnerNOC, Inc,
P.O. Box 29492
Columbus, OH 43229
gpoulos@enernoc.com

Brian Bowen
Regulatory Affairs Manager
FirstFuel Software, Inc.
18 S Michigan Ave, 12th Floor
Chicago, IL 60603
bbowen@firstfuel.com

Mathias Bell
Manager, Regulatory Affairs
Opower, Inc.
1515 North Courthouse Road
Arlington, VA 22201
Email: mathias.bell@opower.com

Merissa Khachigian
Oracle
Director, State Government Affairs
merissa.khachigian@oracle.com