BEFORE THE 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	:	

INITIAL COMMENTS OF C3 IOT

C3, Inc. d/b/a C3 IoT ("C3 IoT") respectfully submits the following Initial Comments in response to the questions posed by the Illinois Commerce Commission ("ICC" or "Commission") in its Notice of Inquiry regarding the Regulatory Treatment of Cloud-Based Solutions.

I.

INTRODUCTION

C3 IoT is a leading provider of cloud-based Software as a Service ("SaaS") and Platform as a Services ("PaaS") solutions to the world's leading utilities and energy companies. We offer an integrated enterprise data analytics platform that harnesses the power of big data, social networking, cloud computing, human-computer interaction models, and machine learning to realize advances in the safety, reliability, cost efficiency, and security of power generation and delivery. On top of this integrated platform, C3 IoT has developed a suite of applications that address business processes across the value chain.

The electric utility industry in Illinois is facing many of the same challenges that utilities globally are experiencing. A combination of rising electric rates, pressure on coal-fired generation, growing renewable energy deployment, and increasing consumer choice and competition, is straining the utilities' business model and operational capabilities. However, these challenges also present opportunities for Illinois' electric utilities to improve their relationship with customers and optimize their operations across the value chain in a way that will deliver significant value to electricity customers. For example, based on a McKinsey & Company report on the value of smart grid analytics applications for Exelon (commissioned by C3 IoT and attached to these Comments as Exhibit A), C3 IoT estimates that deploying the full suite of its SaaS applications across Illinois' approximately 5.1 million electricity customers would deliver $1.24 billion ($243 per customer) in annually recurring economic value to the State of Illinois, in the form of reduced energy bills, more reliable power, and lower CO_2 emissions. In C3 IoT's experience, the only viable approach for the utility industry in Illinois to cost-effectively deploy, operate and benefit from smart grid applications is through effective partnerships with cloud-based service and platform providers.

Taking an enterprise, cloud-based platform approach results in significant cost savings relative to deploying multiple independent on premise point software applications. To estimate the magnitude of these savings, consider a large utility with 10 million customers and three different operating companies.

In order to create a comprehensive smart grid analytics capability across the value chain, the utility might need to procure and deploy five different analytics applications. Examples of five such applications are: (1) revenue protection to detect electricity theft; (2) AMI operations to optimize smart meter deployment and network operation; (3) predictive maintenance to prevent asset failure and enhance operational and capital planning; (4) voltage optimization to reduce overall system voltage; and (5) outage management to enable faster response to and better recovery from system outages.

Leveraging the capabilities of cloud-based applications built on a common data platform, compared to deploying on premise solutions, yields significant cost efficiencies. With respect to a hypothetical deployment of only five high-value utility applications described above, C3 IoT estimates that significant up-front and ongoing costs, in the range of $69 to $189 million over five years, can be avoided by taking a cloud-based, platform approach instead of deploying multiple on premise applications. These cost savings result from lower cost application and data integration costs; avoided hardware and software infrastructure costs; lower ongoing maintenance, support, and operations costs; and avoided procurement expenses. This estimate is not just theoretical: examples of cloud-based smart grid analytics applications built on a common, enterprise data platform exist in large-scale production today at utilities outside of Illinois, such as BGE, PG&E, Enel and ENGIE. By adopting cloud-based enterprise platforms, Illinois' utilities stand to reap significant cost savings as they simultaneously capture value from the increasing volume of data on the grid.

Lastly, as compared with legacy on premise utility technology solutions, the cloud offers unmatched system scalability and data security, combined with lower overall cost of ownership. Proven cloud services providers, such as C3 IoT, implement rigorous cyber security programs to protect critical systems and information assets, constantly monitoring and improving applications, systems, and processes to meet the growing demands and challenges of security. And today's major cloud infrastructure providers, such as Amazon Web Services, deliver significant security benefits because their hundreds of customers derive shared benefits from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations, including the National Security Agency and the Department of Justice.[1] Those cloud infrastructure providers provide hundreds of tools and features to help utility customers meet security objectives around visibility, auditability, controllability and agility, meaning they can meet or exceed utility company security requirements, but without the capital outlay, and with a much lower operational overhead than in on premise environments.

[1] http://www.logicworks.net/blog/2015/06/government-cloud-public-sector-aws-amazon/

II.

RESPONSES OF C3 IOT TO THE COMMISSION'S QUESTIONS REGARDING CLOUD VS. ON PREMISE IT SOLUTIONS

A. Cost:

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

Traditional on premise IT systems have a higher total cost of ownership (TCO) and a much higher up-front cost than cloud-based solutions.[2] The higher upfront costs consist of hardware and software infrastructure that utilities must purchase before an on premise IT system is deployed, and the extensive services, typically purchased from IT systems integrators, required to install an on premise IT system. The utility is also responsible for IT staffing, hardware and software (virtualization and management) maintenance costs. In addition, the utility must bear the cost and timing risks of installing an on premise system. These risks can be substantial, with more than 40% of on premise IT installations over budget and behind schedule.[3] As described below in detail, the 5-year TCO of a cloud-based platform solution at a large utility is estimated to be $189 million lower than that of on premise solutions, $120 million of which is due purely to deploying a software-as-a-service (SaaS) solution in the cloud instead of on premise.

Taking an enterprise, cloud-based platform approach results in significant cost savings relative to deploying multiple independent on premise point software applications. To estimate the magnitude of these savings, consider a large utility with 10 million customers and three different operating companies. In order to create a comprehensive smart grid analytics capability across the value chain, the utility might need to procure and deploy five different analytics applications. Examples of five such applications are: (1) revenue protection to detect electricity theft; (2) AMI operations to optimize smart meter deployment and network operation; (3) predictive maintenance to prevent asset failure and enhance operational and capital planning; (4) voltage optimization to reduce overall system voltage; and (5) outage management to enable faster response to and better recovery from system outages.

The following analysis illustrates that **the cost savings of deploying and maintaining an integrated family of applications built on a common, enterprise, cloud-based platform relative to deploying five independent on premise point applications is up to $189 million over five years ($120 million of which is purely from the cost savings associated with deploying software-as-a-service (SaaS) in the cloud instead of on premise)**. The models and assumptions have been validated with IT operational and financial executives across numerous global utilities.

---

[2] Barbara Vergetis Lundin, "The economics of enterprise smart grid analytics," SmartGridNews (http://www.smartgridnews.com), April 21, 2015.

[3] http://www.prnewswire.com/news-releases/new-survey-results-show-cloud-based-bi-satisfaction-outpaces-on-premise-bi-according-to-business-intelligence-pros-224290661.html

These cost savings accrue from four areas: (1) data integration and implementation, (2) hardware and software infrastructure and services, (3) hardware and software maintenance, support, and operations, and (4) procurement of the solutions and support hardware and software.

1. Data Integration and Implementation

In the coming years, companies will spend more on application integration than on new application systems.[4] A platform approach minimizes these integration costs. Deploying an integrated family of applications that share a common data architecture and cloud-based platform enables a utility to perform a single initial integration without having to repeat the work with the addition of new applications. A platform approach also provides the benefit of being able to flexibly deploy applications either at one time or sequentially over time with little to no incremental effort or cost.

By contrast, deploying independent point applications from different vendors with different architectures and data structures requires a new repeated integration and implementation project for each application. Further compounding the complexity and expense is the need to build integrations between applications to enable *cross-application* data interactions. The cost of performing these integrations for point applications grows quickly because of the rapid growth of the number of unique integrations required. It also results in duplicative and error-prone additional effort.

In summary, the integration cost associated with each additional platform application **decreases** as additional applications are added, whereas the integration cost of each point application **increases** as additional point applications are added.

Recent experience has shown that deploying a single smart grid analytics application, whether on a platform or not, requires approximately 25 data source extracts. Adding four more applications on a platform typically requires only an additional 25 data source extracts for a total of 50. Many data sources are shared by different applications on the platform and all of the data are available to all applications deployed on the platform, which results in the minimal number of total extracts.

By contrast, for independent point applications from different vendors, each application requires 25 separate data source extracts for a total of 125. In addition, applications typically must communicate with each other. On a platform, this communication occurs automatically. However, even a single integration point between each independent application requires an additional 10 (= 4 + 3 + 2 + 1) integrations, for a total of 135 integrations (See Figure 1). Therefore, the cost of integrating five independent point applications is nearly three times higher than that of integrating five applications on a common platform.

[4] Benoit J. Lheureux et al., "Predicts 2015: Digital Business and Internet of Things Add Formidable Integration Challenges." Gartner, November 11, 2014.

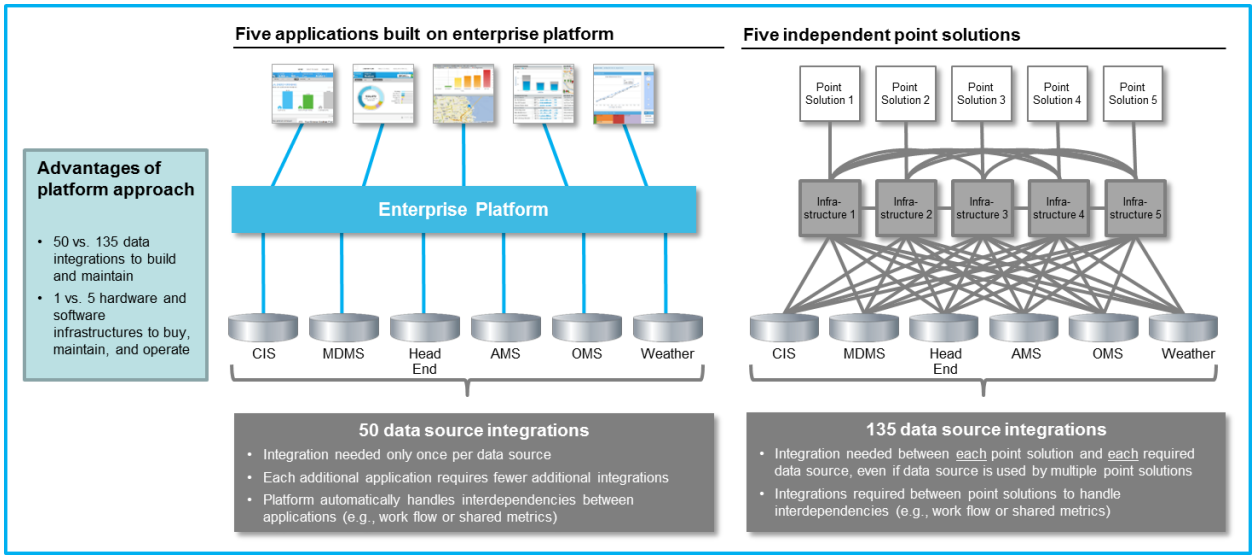

Figure 1. Comparing the integration effort associated with deploying five integrated applications built on an enterprise data analytics platform with the effort associated with deploying five independent point applications from different vendors.

2. Hardware and Software Infrastructure and Services

The platform approach, delivered as Software-as-a-Service (SaaS), provides a single complete and fully functional hardware and software infrastructure at no additional cost. The infrastructure and services included in the SaaS model encompass all necessary facilities, equipment, technologies, and administrative personnel needed to run the system, including security, data center, power, hardware, storage, backup, monitoring, maintenance, and support resources.

By contrast, each independent point solution requires its own hardware and software infrastructure, whether deployed on premise or in the cloud (See Figure 1). In a scenario in which multiple independent applications are deployed on premise, each utility operating company incurs the full infrastructure and service costs for purchasing, integrating, and maintaining multiple hardware (e.g., servers, routers, switches, storage) and software (database management systems, ETL software, etc.) infrastructures. These additional infrastructure and service costs are directly proportional to the number of applications deployed.

3. Hardware and Software Maintenance, Support, and Operations

The SaaS platform approach also provides ongoing maintenance, support, and operations at no additional cost. The incremental internal utility IT personnel requirements are minimal because the applications share the same infrastructure, data model, analytics platform, and user interface.

By contrast, each of the individual on premise solutions incurs fees for hardware and software infrastructure maintenance and support (such as database license support and maintenance) as well as costs for internal IT personnel required to set up and operate the systems. The vendor fees increase in

proportion to the number of individual applications. Additional operations and maintenance expenditure is required, including vendor software upgrades, dealing with hardware issues, internal user requests, de-conflicting multiple incompatible versions, and more costly vendor management. Because of the ever-increasing complexity associated with adding additional point applications, as described in the data integration section, the utility's internal IT operations costs increase faster as more applications are added.

4. Procurement of Applications and Support Hardware/Software

Deploying an integrated family of cloud-based applications across multiple operating companies requires only a single procurement process for the platform.

By contrast, a separate procurement process must be completed for each vendor providing a point application, as well as for each set of hardware and software infrastructure systems required to run these independent applications. The procurement costs can include writing RFPs, assessing responses, negotiating pricing and contract terms, and professional service fees. The procurement cost is directly proportional to the number of applications. To model this cost, we conservatively assume that multiple operating companies within a single corporate structure carry out centralized procurement processes, but experience has shown that is not always the case.

Figure 2 summarizes the cost components described above and shows mathematically how the costs grow as applications and operating companies are added to the deployment.

Cost categories and scaling comparison of Enterprise Platform vs. Individual Point Solutions

	Cost category	Description	Scaling with Enterprise Platform	Scaling with point solution
1	Data Integration and Implementation	Cost incurred by utility for solution development and integration. The costs include configuration, data integration, and additional software development. Implementation timeline estimate is 12 months for a point solution vs. 3-6 months for each Enterprise Platform application.	$W \cdot N \left[\frac{1-A^M}{1-A}\right]\left[\frac{1-A'^O}{1-A'}\right]$	$O \cdot W \cdot N \cdot M \left[1 + B\left(\frac{M-1}{2}\right)\right]$
2	Hardware and Software Infrastructure Services	Cost incurred by utility for hardware infrastructure (servers, routers, switches, storage) and software (relational database management system, distributed key value store, data integration tools, business intelligence tools)	Included in SaaS/PaaS License Fee	$O \cdot X \cdot M$
3	Hardware and Software Maintenance, Support, and Operations	Cost incurred by utility to operate, maintain, and support hardware infrastructure and software solutions. Includes personnel to support software upgrades, hardware issues, internal user requests, and vendor management.	$T\left[\frac{1-C^{O \cdot M}}{1-C}\right]$	$O \cdot Y \cdot M \left[1 + D\left(\frac{M-1}{2}\right)\right]$
4	Procurement	Cost incurred by utility to write RFPs, assess responses, negotiate contract terms, and pay for professional services	U	$O \cdot Z \cdot M$

Legend

O = # of operating utilities	W = cost per integration
M = # applications	X = H/W and S/W cost per application
N = # integrations per application	T = Incremental utility IT personnel for platform solution
B, D are scaling factors for inter-application integration complexity	Y = HW & SW maintenance cost per application
A, A', C are scaling factors for platform synergies	Z = Procurement cost per point solution
	U = Procurement cost for Platform

Figure 2. A platform generates cost savings compared to point solutions through reduced (1) integration; (2) hardware and software infrastructure; (3) hardware and software maintenance, support, and operations; and (4) procurement costs.

The scaling factors B and D described in Figure 2 determine the degree of interdependency between individual point solutions, and therefore the extent to which data integration and ongoing

maintenance costs grow as the number of applications grow. Mathematically, they determine the strength of the growth as a function of the square of the number of applications.

The scaling factors A, A', and C determine the degree of synergy between the applications within an integrated, cloud-based, enterprise platform, and therefore the extent to which data integrated for one application can be used for another application. Mathematically, they determine how quickly the total cost of each additional application decreases relative to the previous application.

Deployment Scenarios

Imagine two scenarios in which a large energy company deploys smart grid analytics applications across three utility operating companies with approximately 10 million customers. In one scenario, the company deploys an integrated family of smart grid analytics solutions built on an enterprise, cloud-based platform. In the other, it deploys five independent on premise smart grid analytics applications from different vendors, each with its own hardware and software infrastructure.

Table 1 compares the five-year costs (not including the software licensing fees of the applications themselves) between the two scenarios and shows a difference of approximately $189 million.

Additional costs accrue due to the much higher execution risk for each individual application deployment relative to the platform deployment. There is a substantial risk of failure or underperformance of on premise hardware/software deployments. In a cloud-based deployment, the risks associated with application integration, development, and deployment are mitigated by the nature of the cloud services contract. The utility pays for performance of the application on an as-you-go basis, and therefore the provider is accountable for ongoing success and performance of the service.

Assuming a 25% risk of failure for the point solutions collectively, compared to a 5% risk of failure for the cloud-based enterprise platform, the value of the lower risk is approximately $49 million, yielding a risk-adjusted total cost savings of $238 million.

	Scenario 1: Cloud-Based Platform Solution	Scenario 2: On Premise Solutions
1. Application and data integration costs	$5,313,905	$22,320,000
2. Hardware and software infrastructure	$0	$69,600,000
3. Hardware and software maintenance, support, and operations	$999,969	$97,020,000
4. Procurement expenses	$1,000,000	$7,500,000
TOTAL	**$7,313,875**	**$196,440,000**
Risk of failure	5%	25%
Cost of risk	$365,694	$49,110,000
TOTAL RISK-ADJUSTED COST	**$7,679,569**	**$245,550,000**

Table 1. Comparison of costs of deploying an integrated family of cloud-based, smart grid analytics applications built on a common, enterprise data platform with that of deploying and maintaining multiple, independent, on premise software applications.

Further Considerations

Cloud-based solutions typically have much higher application and technical performance than on premise solutions. In addition, instead of having to purchase the full capacity of hardware and infrastructure to match the peak computing and storage loads of applications, a utility can rely on the incremental scalability and per-use cost model of cloud computing and storage without paying for that maximum capacity.

<u>ICC QUESTION</u>: 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.

C3 IoT is familiar with at least one large global utility that, in addition to deploying C3 IoT cloud-based solutions, is closing 23 data centers and migrating over 1,200 on premise applications to the public cloud over a period of 12-18 months. The IT cost savings expected are over 25% and the result is a more flexible (immediate increases and/or decreases in compute and storage), reliable and secure compute infrastructure.

The costs associated with migrating utility data systems to cloud services primarily consist of the effort required from technical resources to extract, transform, and load data from legacy on premise systems to cloud-based systems. C3 IoT has completed over 15 of these projects with very good results. It typically takes 2-6 months to migrate data from on premise IT system to a cloud solution, at a cost of $1-2 million, which includes defining requirements; data extraction, mapping, transformation, and loading; software configuration; and quality assurance and testing.

Examples of utility services that have migrated from utility-owned on premise systems to cloud services include:

- Transmission and distribution maintenance systems
- Smart meter operations systems
- Revenue protection systems
- Customer information and billing systems
- Customer relationship management systems
- Facility energy management systems
- Customer engagement and energy management systems
- Energy efficiency web portals

ICC QUESTION: **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.**

The costs associated with training employees to use cloud-based solutions are typically substantially lower than costs to train employees to use utility-owned, on premise systems. This is because modern cloud-based, SaaS and mobile software is typically developed using the latest consumer-oriented human/computer interaction models and user experience paradigms, which results in an easier-to-use, more intuitive software product which utility employees can learn to use more quickly and integrate into their daily business processes. In addition, upgrades and fixes in response to user feedback can be delivered much more frequently (i.e. weekly or monthly updates) than for traditional on premise software systems which operate with 12 – 18 month upgrade cycles.

ICC QUESTION: **Describe whether and how operations and maintenance costs differ between utility-owned, on premise systems and cloud services.**

The operations and maintenance costs of public cloud services are substantially more economical than those of utility owned, on premise systems. This is a result of the dramatically larger scale of the public cloud operations (order of millions of virtual machines) when compared to typical utility owned on premise systems. The economies of scale delivered through public clouds come from standardization of computer hardware and software and significant investments in automated data center monitoring and operations.

Operations and maintenance are typically included in the subscription software license of a cloud service, so the explicit operations and maintenance costs associated with a cloud service are dramatically lower than for on premise systems. In addition, the internal labor costs to the utility of operating and maintaining a cloud system are also dramatically lower because all of the hardware and software infrastructure, operations, monitoring, patching, upgrades, and security are provided and managed by the cloud services provider. Finally, the economies of scale associated with the standardized hardware and software, and standard operations processes that cloud-based solutions utilize are significant. As shown in the answer to question A.1 above, the total cost of ownership, taking into account operations and maintenance costs, is much lower for a cloud solution than a traditional on premise solution.

B. Reliability:

ICC QUESTION: Describe whether and how cloud-based solutions improve safety and reliability at a utility.

Cloud-based solutions can significantly improve safety and reliability at a utility, for two reasons:

1. In order to significantly improve safety and reliability at a utility, software applications must be able to integrate, correlate, analyze, and visualize utility data across enterprise and operational systems in real time or near real time to enable operators and systems to take rapid action if necessary. These applications can only be cost-effectively deployed and operated in the cloud, given the extreme computing and storage resources required. Examples of cloud-based solutions that improve safety and reliability at a utility include:

    - **Predictive Maintenance**. Improves reliability by predicting and avoiding outages due to grid asset or system (i.e. feeders) failures. Minimizes operational and capital expenditures through targeted monitoring of network assets and optimally scheduling maintenance or replacement.
    - **Grid Investment Planning**. Enables grid operators to maximize reliability, safety, and customer satisfaction outcomes of grid investment decisions.
    - **Load Forecasting**. Enables optimized system planning and improves system reliability by better predicting load and mobilizing demand-programs to reduce and shift peak load.
    - **Outage Analysis, Prediction & Restoration**. Improves safety and reliability and reduces operational expense by providing analysis of ongoing grid operations, external risks, and outage events and enabling enhanced preparation for and response to both equipment-related and weather-related outages.
    - **Grid Cybersecurity**. Connects cyber threats with operational vulnerabilities to deliver actionable insights on key cybersecurity threats.

2. Cloud solutions provide superior cybersecurity, and therefore better safety and reliability, as discussed in the cybersecurity section below.

Proven Cloud Technologies in Regulated Utilities

i. **<u>ICC QUESTION</u>: 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.**

The market-leading public cloud and virtual private cloud service providers (such as Amazon Web Services) have proven to be most successful at public utilities. C3 IoT has deployed applications at over 15 utilities that are all extremely successful in the areas of customer engagement, energy use analytics, and energy efficiency; smart meter operations; theft detection and prevention; and predictive maintenance of generation, transmission, and distribution assets.

The difference between public and private clouds is as follows:

A public cloud is operated in one or more data centers by an infrastructure provider such as Amazon Web Services, Google Cloud, or Microsoft Azure and is available for use by any customer. Public cloud providers have large scale and best-in-class operational expertise and security that enable the lowest cost, most scalable, secure and reliable service. Public clouds also provide extended redundancy and disaster recovery capability through multiple geographically dispersed data centers.

Note that public cloud providers also provide "virtual private clouds" which are physical and logical subsets of the data center that provide all of the features of a private cloud (data and physical isolation) that a physical private cloud provides, at the low cost, scalability, security and reliability of a public cloud.

A private cloud is a physically separate environment in which the hardware, storage and network are dedicated to a single client or company, and often has been custom-built using proprietary technology. A utility's IT managers are responsible for managing the private cloud. As a result, private cloud deployments carry all of the staffing, management, maintenance, and capital expenses associated with traditional on premise deployments.

Both public and private clouds can be used by the utility industry, but the public cloud provides cost and scalability advantages that a private cloud does not, while at the same time providing higher levels of reliability, security and compliance.

ii. <u>ICC QUESTION</u>: Identify public utilities that have adopted cloud-based solutions and what effect cloud services have had on the utility's safety and reliability.

Many public utilities globally and in the United States have adopted cloud-based solutions, including the more than 15 utilities globally that have deployed C3 IoT cloud-based solutions. Examples of utilities that have deployed C3 IoT cloud-based solutions include (but are not limited to):

- Enel
- ENGIE
- Pacific Gas & Electric
- San Diego Gas & Electric
- Entergy Arkansas
- Westar
- Baltimore Gas & Electric
- Eversource (Connecticut Light & Power, NSTAR, WMECO, Yankee Gas)

Deploying cloud-based solutions has increased these utilities' safety, efficiency, and reliability by:

- Predicting failures on transmission and distribution assets, which improves reliability
- Predicting failures on renewable and conventional generation assets, which decreases cost and improves reliability and safety
- Reducing customer energy use (and therefore wear and tear on assets)
- Reducing distribution technical line losses
- Reducing cost of operating smart meter networks by predicting failures
- Preventing smart meter failures, including dangerous overheating-related issues
- Reducing energy theft
- Reducing tampering on gas meters, which improves safety and reliability

In all cases, deploying these cloud-based solutions resulted in meeting or exceeding the safety, reliability, and operational efficiency targets agreed to with the utility prior to deployment.

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

The majority of utility enterprise systems could be operated more reliably, more securely and at lower cost through virtual private deployments on public cloud infrastructure. Other operational systems required to operate the power grid (e.g.,. infrastructure control or SCADA systems) could be maintained close to the network infrastructure to minimize latency and separate from the corporate intranet or public internet.

This approach is proven to work effectively. For example, a large global utility recently consolidated 1,700 on premise systems to 1,200 and moved all of these systems and Smart Grid Analytics systems to the public cloud. The remaining on premise systems were related to network automation and network control (e.g., SCADA systems).

<u>ICC QUESTION</u>: 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.

Many industries have adopted cloud services with great success, including the following highly regulated industries, either for specific use cases or across their value chains:

- Financial services (e.g., fraud detection and prevention)
- Airlines (e.g., aircraft safety and reliability)
- Rail (e.g. collision prevention)
- Oil and gas (e.g. predictive maintenance for well blowout preventer)
- Refineries (e.g., predictive maintenance for distillation column)
- Auto manufacturing (e.g., factory equipment predictive maintenance)
- Pharmaceuticals (e.g., safety compliance and prescription drug tracking systems)
- Health Care (e.g., health predictive analytics, health insurance fraud)
- Federal Government (e.g., Cybersecurity analytics, surveillance)

Examples of cloud based software deployments have been compiled by Gartner[5] and a survey of businesses commissioned by Microsoft.[6]

Industry analysts believe that there is a trend toward using cloud computing for all enterprise

[5] https://www.gartner.com/doc/1761616/case-studies-cloud-computing.
[6] http://cdn.itcontenthub.com/wp/57275/57275.pdf.

software and that by 2020 over 60% of office software will be in the cloud.[7] The reason for this trend is clear; the cost savings, scalability, reliability and redundancy, better security, and operational simplicity offered by cloud providers. In addition, connected devices and products (commonly referred to as the "Internet of Things") will play an increasingly important role in business operations. Analysis by leading industry experts, such as Michael Porter of Harvard Business School and McKinsey & Company shows that cloud-based IT systems are critical for enabling the Internet of Things.[8]

C. Cybersecurity:

1. Cloud Security

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

Utilities will benefit significantly from the cybersecurity practices provided by established cloud-based solutions providers versus those associated with on premise solutions, primarily because cloud-based solutions providers have invested significantly to implement rigorous cybersecurity practices, in the form of technical, physical, and administrative safeguards, than utility IT departments. Cybersecurity is core to the business model of cloud providers, and they therefore have invested heavily, have hired and trained leading cybersecurity experts, check their networks every second for intrusions, are not susceptible to intrusions delivered through USBs or e-mail attachments and are first to adopt new security practices and technologies as they become available.

ii. ICC QUESTION: Identify any cybersecurity benefits of using a cloud-based solution versus an on premise IT system.

The cybersecurity benefits of using a cloud-based solution versus an on premise IT system include:

- Lower risk of physical security breach since cloud-based solutions are hosted in data centers with state-of-the-art facility security and limited physical access.
- Lower risk of cybersecurity breach due to technical incursion because of advanced data security and network security measures, continuous monitoring, and robust business continuity measures. For example denial-of-service attacks are much more difficult to achieve on a large public cloud service provider because of the ability to re-assign capacity.[9]
- Lower risk of personnel-caused cybersecurity breaches due to robust administrative safeguards (secure design and engineering, data governance, access rights, and compliance).

---

[7] "Forecast Analysis: Enterprise Application Software, Worldwide", 2015, Gartner.

[8] See Michael E. Porter and James E. Heppelmann, "How Smart, Connected Products Are Transforming Competition," Harvard Business Review, November 2014 and McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype," June 2015.

[9] https://aws.amazon.com/security/introduction-to-cloud-security/

All of the benefits described above result in a much lower likelihood of a cybersecurity incident at a utility. Note the widely publicized data breaches have occurred at corporate or government data centers rather than public cloud providers.

Further details can be found in many publications, including for example, a comprehensive overview by Amazon Web Services.[10]

2. New Risks
   i. **<u>ICC QUESTION</u>: Describe the extent of new risks introduced (if any) when a utility migrates to a cloud-based solution from an existing on premise system.**

      In our experience there are no new risks introduced when a utility migrates to a cloud-based solution from an existing on premise system. On the contrary, as discussed above, risks are significantly reduced.

3. Incident Response
   i. **<u>ICC QUESTION</u>: Describe how cloud-based solution providers can respond to cybersecurity threats in contrast to utilities utilizing on premise systems.**

      There are two ways in which cloud-based solution providers can respond to cybersecurity threats in contrast to utilities utilizing on premise systems:

      1. Cloud-based solution providers are constantly monitoring the system for cybersecurity threats using sophisticated tools, and can therefore respond to and mitigate cybersecurity threats very quickly.

         A major benefit of utilizing virtual private cloud / public cloud infrastructure is the inclusion of dedicated personnel and advanced tools for the monitoring, detection, and prevention of cyber vulnerabilities and incidents. Cloud providers are equipped with 24-hour monitoring systems and control room personnel specialized the detection and proactive defense against cyber vulnerabilities. Using these shared personnel and tools allows cloud vendors to provide higher levels of cyber / IT systems defense against intrusion and vulnerability than typical utility on premise systems. Physical security is enhanced through use of cloud infrastructure, and in addition the policies, procedures, and staffing of cloud infrastructure systems generally means that response and recovery from cybersecurity incidents is faster than an on premise system where likely only a handful of personnel (working during business hours) is available to fully address such issues.

      2. Cloud-based solution providers provide cybersecurity applications that directly identify cybersecurity threats by analyzing both operational and IT threat data and performing sophisticated machine learning to predict threats. It is challenging and expensive to perform these big data, complex computations except in the cloud.

[10] https://aws.amazon.com/security/

In summary, public cloud providers spend significantly more than utilities to ensure the security of their data centers.

4. Threat Detection

   i. **<u>ICC QUESTION</u>: Describe whether and how a cloud-based solution can assist a utility in protecting, detecting, and responding to cybersecurity threats and operational vulnerabilities.**

   Cloud-based cybersecurity solutions, like C3 IoT Grid CyberSecurity, are very effective in assisting utilities in protecting, detecting, and responding to cybersecurity threats and operational vulnerabilities. The solutions provide utility cybersecurity teams with advanced diagnostics and predictive tools to identify, prioritize, and reduce the risks of grid cybersecurity vulnerabilities. Utility operators are able to quickly prioritize security resources to address the network and grid assets that have the most significant potential impact on operational safety, reliability, and integrity. By enabling earlier and more rapid resolution of high priority vulnerabilities, these solutions prepare operators with advance warning and lead time to address and remediate at-risk equipment and networks.

   Cloud-based cybersecurity applications support utility operators by merging two key views of the network and grid to create a comprehensive risk assessment: 1) hardware and software vulnerability metrics for individual assets, and 2) the operational and customer-facing and impacts of potential asset security breaches. By combining these two traditionally separate views, cybersecurity teams and utility operators are provided with a bottom-line prioritization that helps sort through the critical actions needed to maintain and improve network integrity.

   A major benefit of utilizing virtual private cloud / public cloud infrastructure is the inclusion of dedicated personnel and advanced tools for the monitoring, detection, and prevention of cyber vulnerabilities and incidents. Among other things, cloud providers are equipped with 24-hour monitoring systems and control room personnel specialized in the detection and proactive defense against cyber vulnerabilities. Using these shared personnel and tools allow cloud vendors to provide higher levels of cyber / IT systems defense against intrusion and vulnerability than typical utility on premise systems. Physical security is enhanced through use of cloud infrastructure, and the policies, procedures, and staffing of cloud infrastructure systems result in a faster response and recovery from cybersecurity incidents than for an on premise system, where only a handful of personnel (working during business hours) are available to fully address such issues.

5. Security Framework for Utilities

   i. **<u>ICC QUESTION</u>: Identify the key elements and value of a security best-practices framework for utilities to address cybersecurity threats.**

   By way of example, the following describes C3 IoT's security program. C3 IoT recommends that utilities adopt many of the same best practices to address cybersecurity threats. The C3 IoT Cyber Security Program is a multi-layered

security approach that employs technical, physical, and administrative safeguards.

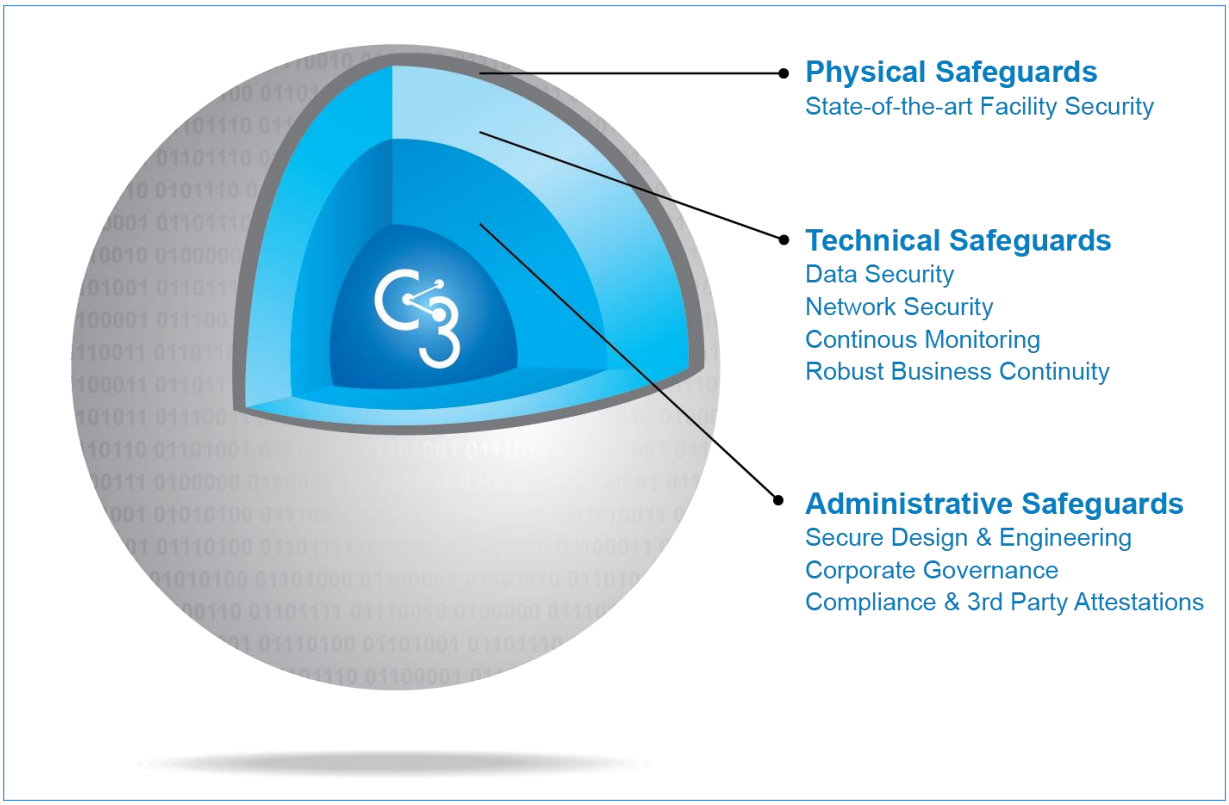

Figure 3: C3 IoT Cyber Security Program's multi-layered security approach.

The C3 IoT Cyber Security Program has been developed to comply with all applicable legal and regulatory requirements, including compliance with the NERC CIP smart grid cyber security standards.[11] This program encompasses a comprehensive set of cyber security controls and business processes based on NIST best practices that align with the NERC CIP standards.

Physical Safeguards

- ***Physical and Operational Security:*** C3 IoT combines state-of-the-art data center facilities with industry best practices to ensure operational security.

Technical Safeguards

- ***Network Security:*** C3 IoT provides Virtual Private Clouds accessible over robust network infrastructure to provide secure and reliable systems.

[11] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- ***Data Security:*** Data security is a fundamental requirement that is systematically addressed throughout the C3 IoT Analytics Engine. This includes access controls, encryption, user roles, data retention/destruction, and regulatory compliance.

- ***Continuous Monitoring:*** C3 IoT uses multiple, redundant, continuous monitoring systems application and data security.

- ***Business Continuity:*** C3 IoT backup, failover, and redundancy services ensure data availability and protect information from loss or destruction.

Administrative Safeguards

- ***Secure Design and Engineering Principles:*** C3 IoT follows best practice secure software development processes to incorporate security throughout the product development and release lifecycle.

- ***Corporate Governance:*** Cyber security is a strategic priority for C3 IoT. C3 IoT has implemented extensive corporate oversight to ensure its ongoing success.

- ***Third-Party Attestations:*** C3 IoT offers a variety of third-party attestations regarding cyber security processes and controls.
    - C3 IoT undergoes regular testing by external security experts, including source code reviews, software vulnerability testing, and penetration testing.

    - C3 IoT uses data centers that have been audited for the leading industry IT security standards, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, International Traffic in Arms Regulations (ITAR), and FIPS 140-2.

ii. <u>ICC QUESTION</u>: Identify the security best-practices framework you would recommend for Commission adoption and explain why.

Please refer to answer to 5.i.

6. Security Framework for Cloud Providers

i. <u>ICC QUESTION</u>: Identify the key elements and value of standardized security requirements for cloud-based solution providers.

As an example of a cloud provider's security processes please see:

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

An excerpt of AWS's compliance program is provided below:

AWS Compliance Program
Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

ii. <u>ICC QUESTION</u>: 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 premise systems.

Please refer to answer to 6.i. As demonstrated above cloud services can afford to comply with a significantly broader set of security standards and best practices than on premise data centers.

iii. <u>ICC QUESTION</u>: 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 premise solutions.

Please refer to answer to 5.i.

iv. **<u>ICC QUESTION</u>: Identify the cloud services selection guidelines you would recommend for Commission adoption and explain why.**

Please refer to answer to 5.i.

7. Best Practices

i. **<u>ICC QUESTION</u>: Describe how best practices in protecting sensitive utility and customer information differ between cloud-based hosting and on premise hosting.**

Please refer to answer to 5.i. and 6.i. Utility and customer information is more secure on public cloud infrastructures than in on premise utility data centers.

8. Compliance

i. **<u>ICC QUESTION</u>: Describe whether and how cloud-based solutions can improve utility compliance, privacy, and data security.**

By leveraging the enhanced network and data security practices inherent in the leading cloud-based solutions, utilities will find it easier, faster and less expensive to meet baseline and evolving compliance requirements. Cost-savings and efficiencies garnered by utilities from deploying cloud-based solutions are then available to address compliance, privacy and data security issues related to human factors, business processes and non-technical risk.

9. What Should Utilities Avoid Putting in the Cloud?

i. **<u>ICC QUESTION</u>: 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?**

Because cloud-based services provided better security than on premise systems, utility systems will be more secure on public cloud infrastructures. Exceptions would be infrastructure control systems or SCADA systems which are co-located with grid and generation infrastructure to avoid possible latency and in order to isolate those systems from the corporate intranet or public internet.

10. Connectivity

i. **<u>ICC QUESTION</u>: 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?**

Using a cloud-based application platform with a standard data model across utility functions (i.e. customer, distribution, transmission and generation), disparate, siloed data systems can be integrated and data correlated across those

systems into a unified cloud data image. Those data can be kept current in real-time or near real-time. These data can be leveraged for a large number of applications and use cases including grid asset and generation predictive maintenance, technical and non-technical line loss reduction, and improved customer engagement.

III.

RESPONSES OF C3 IOT TO THE COMMISSION'S QUESTIONS REGARDING REGULATORY BARRIERS

Regulatory Barriers:

A. Ratemaking Treatment:

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

   Yes, current ratemaking practice discourages Illinois utilities from deploying cloud-based solutions (e.g., data analytics) provided by third party vendors. This is because (1) current ratemaking practice incentivizes utilities to spend capital instead of operations and maintenance expense ("O&M"), and (2) utilities are reluctant to capitalize costs associated with cloud-based solutions.

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

   There is no reasonable justification for accounting ratemaking distinction between investing in cloud-based solutions and investing in on premise solutions. Traditional capitalization requirements have typically treated on premise computing hardware and software as a capitalized expense due to the significant up-front and one-time cost of acquiring these items for future benefit. As a result, utilities and ratepayers have had to assume significant costs and risk of such systems. Under a cloud-based model, the ongoing benefits of software are provided, yet without the significant upfront costs. Since in both cases, the utility has the right to use and benefit from the software for similar periods of time, it is reasonable to allow these benefits to be realized by accommodating them as capital expenses, as an extension of traditional accounting treatment.

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

   Some utilities have pursued limited adoption of cloud-based solutions despite the accounting treatment. In our experience, this occurs in one of three ways:

   1. Utility pays for solution using O&M budget, despite the incentive to spend capital. This typically only happens, however, when the utility has a pre-

allocated or approved O&M budget for a specific initiative (e.g., for energy efficiency programs).

2. Utility insists on acquiring a perpetual license for the cloud-based software solution, and capitalizes the perpetual license fee. However many cloud solution providers are highly reluctant to provide perpetual licenses, since this represents a fundamental deviation from the core business model of SaaS, cloud-based solutions.
3. Utility capitalizes the SaaS license fees associated with the cloud-based solution (typically because that utility has a regulatory accounting department that is ahead of the industry at large, and follows the latest U.S. Financial Accounting Standards Board ("FASB") accounting guidelines for the capitalization of cloud-based or hosted software solutions).[12]

Option 3 is the preferred, accounting standards-supported, and economically most rational approach. This option can be encouraged in large part by regulatory support for the capitalization and rate-basing of costs associated with cloud-based solutions.

4. <u>ICC QUESTION</u>: 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 premise 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 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 premise IT systems owned by the utility:

1. Under the current overall ratemaking structure, explicit endorsement by regulatory agencies of the ability for utilities to capitalize cloud-based software solutions. This is simply an endorsement of current FASB accounting guidelines, and assurance that the costs associated with cloud-based solutions will not be treated differently from the costs associated with on premise IT systems when it comes to including these costs in the rate base.

   i. Costs to implement: none
   Benefits: remove the disincentive to deploy the most modern, cost-effective and secure software solutions available, and thereby deliver significant savings and improved reliability to utility customers.

   ii. Illinois administrative rules that would need to be revised, and the revisions(s) required: Unknown

[12] http://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176165941746

2. Move from traditional cost-of-service based ratemaking mechanisms to an incentive-based mechanism such as the RPI-X or RIIO mechanisms used in Europe (see for example https://www.ofgem.gov.uk/network-regulation-riio-model). This would remove the bias toward just spending capital and incentivize utilities to capture the cost efficiencies that advanced cloud-based solutions provide, while also providing a host of additional benefits.

   i. Costs to implement: non-zero. The ICC would better be able to estimate the costs of this option.
   Benefits: Directly incentivize utilities to operate more efficiently, cost-effectively, and reliability. Remove the disincentive to deploy the most modern, cost-effective and secure software solutions available, and thereby deliver significant savings and improved reliability to utility customers.

   ii. Illinois administrative rules that would need to be revised, and the revisions(s) required: Unknown

B. Other Barriers:

1. **ICC QUESTION: 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.**

   There are several other regulatory barriers that discourage Illinois utilities from deploying cloud-based solutions. These are briefly described below.

   1. Data security and data privacy regulations that may be interpreted to give preference to on premise IT systems, even though the cloud is more secure, as discussed above.

   2. Regulatory encouragement of small-scale "pilots" that foster an ever-increasing use of disparate applications. This increases integration and application management complexities and costs. While certain technology pilot projects sometimes result in the eventual production deployment of applications, C3 IoT's experience is that utilities are conducting pilots in lieu of, or delaying, an investment in actual production deployments that deliver operational efficiencies, safety, reliability, and costs savings to Illinois ratepayers. This practice also highlights the industry's lack of knowledge and information sharing between different business areas and with regulators – a challenge that a cloud-based analytics platform would address very effectively.

   3. The lack of true, robust, transparent risk-based asset management frameworks as part of the rate case process. For example, several utilities in the UK and Australia have adopted ISO 55000, the ISO framework for risk, and PAS 55. Such frameworks would encourage utilities to adopt solutions that provide deeper insight into their asset base and operations

that would be best enabled by cloud-based solutions, as described above.

IV.

RESPONSES OF C3 IOT TO THE COMMISSION'S QUESTIONS REGARDING ADDITIONAL BENEFITS OF CLOUD DEPLOYMENT

Additional Benefits of Cloud Deployment:

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

   A wide variety of different cloud-based technologies are available for the full range of business and operational processes for electric, gas, and water utilities, from customer billing to meter management to power generation operations. C3 IoT has developed a powerful data integration, analytics, and application development platform that is available for utilities to develop and deploy advanced analytics and operational applications to enhance the reliability, security, and efficiency of their operations. In addition, C3 IoT has developed a suite of smart grid analytics applications on this platform across the electric, gas, and water utility value chains that improves the safety, reliability, and efficiency of power, gas, and water delivery. These applications can deliver up to $300 per meter of annual economic value to an average US utility and its customers. Examples of the applications available include:

   - Energy efficiency, demand response, and customer engagement analytics and web portals
   - Smart Meter Operations
   - Revenue Protection
   - Predictive Maintenance for networks
   - Grid Investment Planning
   - Voltage and VAR Optimization
   - Outage Analysis, Prediction, and Restoration
   - Grid Cybersecurity
   - Predictive Maintenance for Generation

   Please refer to the answer to Question 4 below for further details on cloud-based solutions available to utilities, and the value they provide to utilities and their customers.

2. **ICC QUESTION: 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 premise and cloud solutions, or is only one option available?**

      C3 IoT provides the following specific software services to engage customers in distributed generation, distributed storage, demand response, and energy efficiency programs for electric utilities. These services are available only as

cloud solutions. With the exception of residential energy efficiency portals (described below), C3 IoT does not believe that these software services are currently deployed in Illinois, despite their availability.

Distributed Resource Management. Provides actionable insights on assets and programs that influence energy demand and supply from the customer-side, including distributed generation, distributed storage, electric vehicles, demand response and energy efficiency programs (utility and third-party).

Load Forecasting. Enables optimized system planning and improves system reliability by better predicting load and mobilizing demand-programs to reduce and shift peak load.

Demand Response Analytics. Enables optimized system planning and improves system reliability by better predicting load and mobilizing demand-programs to reduce and shift peak load.

Customer Analytics. Customer engagement portals that help meet regulatory mandates for verified energy savings and demand reduction; help engage customers in distributed generation and storage, demand response, and energy efficiency; improve customer loyalty and engagement; and increase customer satisfaction.

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.

C3 IoT provides the following customer engagement portals that improve customer engagement, increase customer satisfaction, and help meet regulatory mandates for verified energy savings and demand reduction for electric utilities. C3 IoT does not believe that these services are currently deployed in Illinois.

C3 Residential. Customer engagement portal that improves residential customer loyalty and engagement; increases customer satisfaction; and helps meet regulatory mandates for verified energy savings and demand reduction. Enables optimized targeting of the right programs, products, and services to the right customers through the right channel. We note that the C3 Residential software is currently available to some customers in the State of Illinois and is serving to reduce energy bills for Illinois homeowners and renters.

C3 Commercial. Customer engagement portal that improves small and medium business customer loyalty and engagement; increases customer satisfaction; and helps meet regulatory mandates for verified energy savings and demand reduction. Enables optimized targeting of the right programs, products, and services to the right customers through the right channel. Reduces energy bills for Illinois small business owners and operators.

C3 Enterprise. Energy and facility management portal that enables enterprise energy managers to understand, investigate, and benchmark energy use within

and across facilities and to target energy efficiency and demand response projects for maximum energy reduction and economic return.

3. **<u>ICC QUESTION</u>: 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.**

      C3 IoT provides the following software that improves customer engagement and increases customer satisfaction for water and gas utilities. C3 IoT does not believe that this type of software or service is currently deployed in Illinois.

      Customer Analytics. Customer engagement portals that improve customer loyalty and engagement; increase customer satisfaction; and help meet regulatory mandates for verified energy savings and demand reduction. Enables optimized targeting of the right programs, products, and services to the right customers through the right channel.

   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.**

      C3 IoT provides the following software that detects leaks and inefficiencies, improves conservation, and lowers operating costs for water and gas utilities. C3 IoT does not believe that this type of software is currently deployed in Illinois.

      <u>Sensor Health.</u> Identifies and priorities gas or water meter malfunctions and losses. Validates operational functionality and integrity of smart meter networks. Lowers operating costs for meter networks.

      <u>Loss Prevention.</u> Identifies and priorities gas or water theft and leaks in the network. Reduces unbilled gas and water by detecting tampered, bypassed, and malfunctioning meters.

      <u>Predictive Maintenance</u>. Minimizes both operational and capital expenditures through targeted monitoring of network assets, predicting and avoiding service interruptions and leaks due asset failure, and optimally scheduling maintenance or replacement.

4. **<u>ICC QUESTION</u>: 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.**

   Cloud-based solutions can offer enormous benefits to Illinois utilities and their customers. This value accrues both to shareholders of the utility and to the utility's customers. Deploying the full suite of Smart Grid Analytics applications across all of Illinois' approximately 5.1 million electricity customers could deliver $1.24 billion in

annually recurring economic benefit to these customers. This is equivalent of $243 in economic benefit per customer per year.

The table below lists the applications, describes their features and functionality, and summarizes the value they can unlock if deployed across Illinois. The value estimates below are informed by a detailed analysis performed by McKinsey & Company, attached to these comments as Exhibit A.

C3 IoT Products	Functionality	Annual Value
C3 Customer Analytics: C3 Residential™, C3 Commercial™, C3 Enterprise™, C3 Customer Insight™. Customer engagement portals that improve customer loyalty and engagement; increase customer satisfaction; and help meet regulatory mandates for verified energy savings and demand reduction. Enables optimized targeting of the right programs, products, and services to the right customers through the right channel.	• Provide 360 degree view of the customer. • Provide customers direct access to their energy use information. • Generate targeted product and service offerings based on customer profiles and historical usage patterns. • Prioritize actions to save energy based on facility end-uses. • Track savings over time • Performs multidimensional analysis using energy, demographic, firmographic, and propensity data to establish customers segments most likely to engage in buying or other desired behavior	**$335 million** $66/customer
C3 Distributed Resource Management™. Provides actionable insights on assets and programs that influence energy demand and supply from the customer-side, including distributed generation, distributed storage, electric vehicles, demand response and energy efficiency programs (utility and third-party).	• Integrates all enterprise and external data required to identify and visualize distributed resources, including rooftop PV, storage, EV chargers, CHP, and home energy control devices. • Integrates with control solutions within and at the edge of the grid. • Displays location and status of each resource on a grid-wide view. • Analyzes patterns of energy use from individual meters up to large aggregations of customers combined with external data to provide real-time spatial and temporal knowledge of distributed assets. • Analyzes impact on grid voltage and power factor. • Recommends operational and investment actions to take.	**$53 million** $10/meter
C3 AMI Operations™. Validates operational functionality and integrity of the AMI network.	• Applies sophisticated analytics on consolidated data from multiple utility systems to optimize AMI deployment and verification, and to identify malfunctioning meters and poor-quality data.	**$11 million** $2/meter
C3 Revenue Protection™. Reduces unbilled energy by detecting tampered, bypassed, and malfunctioning meters.	• Applies sophisticated analytics on consolidated data from multiple utility systems to identify suspicious energy usage, assign likelihood of non-technical loss, and estimate revenue loss at stake.	**$25 million** $5/meter
C3 Predictive Maintenance™. Minimizes both operational and capital expenditures through targeted monitoring of network assets, predicting and avoiding outages due asset failure, and optimally scheduling maintenance or replacement.	• Monitors, detects, and diagnoses distribution asset parameters (dynamic loading, capacity optimization, and voltage abnormalities) in real-time. • Integrates AMI data with OMS, WAM, GIS, and CIS data systems to proactively identify and address assets at risk of failure.	**$110 million** $22/meter
C3 Grid Investment Planning™. Enables grid operators to maximize reliability, safety, and customer satisfaction outcomes of grid investment decisions.	• Connects grid operations capital projects with asset risk, customer impact, and system reliability indices to build a pipeline of capital and O&M investment projects that achieve desired outcomes in the most capital-efficient manner.	**$134 million** $26/meter
C3 Load Forecasting™. Enables optimized system planning and improves system reliability by better predicting load and mobilizing demand-programs to reduce and shift peak load.	• Analyzes patterns of energy use from individual meters up to large aggregations of customers, combined with external data such as weather, economics, and energy/ technology price trends, to understand and predict load from hourly to yearly timescales and overlays grid constraints with load patterns	**$26 million** $5/meter
C3 Demand Response Analytics™. Enables optimized system planning and improves system reliability by better	• Analyzes patterns of energy use from individual meters up to large aggregations of customers, combined with external data such as weather, economics, and energy/ technology price trends, to understand and	**$54 million** $11/meter

predicting load and mobilizing demand-programs to reduce and shift peak load.	predict load from hourly to yearly timescales and overlays grid constraints with load patterns	
C3 Outage Analysis, Prediction & Restoration™. Improves safety and reliability and reduces operational expense by providing analysis of ongoing grid operations, external risks, and outage events and enabling enhanced preparation for and response to both equipment-related and weather-related outages.	• Identifies high-risk areas of distribution system as a function of asset status (equipment age, load history, temperature) and external factors (vegetation, fire, extreme weather) to proactively address safety and reliability issues. • Optimizes outage response activities by coupling real-time AMI data with historical outage pattern information.	**$197 million** $39/meter
C3 Volt/VAR Optimization™. Reduces operational and capital expense by reducing voltage variations across the distribution network, and lowering/right sizing voltage at feeder sources.	• Uses AMI data, utility distribution topology, outage management systems, and documented engineering constraints to identify the most inefficient feeders, estimate financial savings associated with voltage reduction, and provide feeder remediation recommendations.	**$242 million** $47/meter
C3 Grid Cybersecurity™. Connects cyber threats with operation vulnerabilities to deliver actionable insights on key cybersecurity threats.	• Integrates operational and asset risk data with threat data from IT security systems. • Provides actionable recommendations to mitigate threats with the highest operational and safety implications.	**$53 million** $10/meter
TOTAL		**$1,240 million** $243/meter

IV.

CONCLUSION

C3 IoT appreciates the opportunity to submit these Initial Comments, and looks forward to providing any further information which the Commission and other participants find helpful regarding cloud-based solutions.

Respectfully submitted,

C3, INC D/B/A/ C3 IOT

By: Edward Abbo

Its: President & Chief Technical Officer