

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

**Reliability Technical Conference**                         )  
   )  
   )         **Docket No. AD19-13-000**

---

**PREPARED REMARKS OF DAVID ROSENTHAL  
ON BEHALF OF  
THE MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC.**

---

## **I. Introduction**

Good afternoon, Thank-you Chairman Chatterjee and Commissioners for this opportunity to speak with you on Cloud Services – these are opportunities that can transform our industry and make our systems more reliable, resilient and secure.

Cloud Services are tools to solve problems, no different in that regard from servers, data bases and software – tools we use every day. It is important to recall that there was a time when each of these technologies was new, untested, and not considered “industry standard.” Today it is difficult to imagine how we could do our work effectively and efficiently without these technologies. I believe this is the lens through which we can view Cloud Services. The specifics of how and when we will integrate Cloud Services into our ways of work is a challenge. I thank the Federal Energy Regulatory Commission (“Commission”) for convening this panel to discuss those kinds of details.

At Midcontinent Independent System Operator, Inc. (“MISO”) I spent 8 years as the Director of IT infrastructure managing the entire server, network, storage, telecommunications and desktop environment and, now, as the Director of Incident Response and system recovery I see that we are at a point in the industry where we must look at ways to incorporate the secure, reliable computing opportunity that is Cloud Services.

It is no longer a question of “whether” Cloud Services have a place in our industry; rather, it is a question of when, what, and how Cloud Services will work in our industry. Major software vendors have moved quickly from a “Cloud first” to a “Cloud only” mindset, and that tells us that older, non-Cloud technologies will not be supported indefinitely. Other aspects of Cloud Services (Software as a Service, Platform as a Service, and Infrastructure as a Service) are developing quickly.

As you know the federal government now stores some of its more sensitive information in the Cloud.

At MISO, we are already piloting aspects of Cloud Services internally, with the exception of Operations, NERC and NERC CIP. For example, MISO is building its Security Reference Architecture and piloting with internal groups to determine what needs to be done from a security perspective during each phase of a project lifecycle. To that end, MISO has active pilots engaging “back office” functions like financials and desktop services.

## **II. What is the Cloud**

Cloud Services can mean different things to different people. It is important to establish the working definition for Cloud Services in this context, as a basis for this discussion. The National Institute of Standards and Technology (NIST) offered a good definition of Cloud Services:

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (See Special Publication 800-145 2011).

For NIST and for these comments, the common definition of Cloud focuses on services and not on the technologies that support those services. NIST further defines these Cloud Services in terms of who may access these services. Cloud Services for use by a single organization are generally referred to as Private Cloud. Cloud Services for use by a community of organizations are generally referred to as Community Cloud. Cloud Services for use by anyone are generally referred to as Public Cloud.

NIST has defined the essential characteristics of a Cloud service to include the following:

- On-Demand
- Broad Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

The NIST definitions inform these comments.

### **III. Why Cloud/Benefits of Cloud**

Cloud computing offers many benefits to organizations of all sizes. For example, small organizations can benefit dramatically when comparing the cost of self-hosted solutions to Cloud Services. In our industry, reliability and security are the name of the game; and Cloud Services can offer significant value in these respects as well. I would like to highlight a few specific benefits of cloud computing.

Cloud Services offer redundancy and resiliency of data and systems and with the right security protocols in place can be accessed safely across many devices and locations. Improved access and performance can dramatically increase productivity and bring new products and services to market faster. The rapid scalability of these services to achieve peak needs allows organizations to satisfy business needs in a “pay for what you use” manner. This brings an opportunity for cost savings compared to the legacy practice of procuring and supporting hardware. Furthermore, utilizing infrastructure services from external providers, organizations can transfer previous business risks related to hardware investments and breakdowns to organizations better equipped to handle these challenges. Cloud Services providers can also be better equipped to provide robust security solutions.

Utilizing these services does come with concerns. For example, ensuring availability of these systems is vital; ideally, 100% availability is essential for utilities and grid operators. Placing our systems and data in the cloud entrusts the information to a host of new organizations and individuals that we have less oversight or control over. We must work to ensure our industry can safely navigate a transition to this space.

#### **IV. Current state of CIP and the limitations**

Current NERC Critical Infrastructure Protection (CIP) standards discourages our industry from considering Cloud Services, as those CIP standards were not developed with Cloud Services in mind and they offer no guidance as to whether and how Cloud Services may be NERC CIP compliant. Two concerns typically dissuade this industry from considering Cloud Services:

1. How to securely manage BES Cyber System Information (BCSI) in the Cloud
2. How to securely and reliably manage BES Cyber Systems in the Cloud

The first concern is with information management. How do we ensure that our critical information is not shared inadvertently or purposely with those who may intend to harm us or the bulk electric system, including, for example, “bad actors.” Our industry’s most sensitive information, in the wrong hands, can adversely affect the reliability and resilience of our bulk electric system.

The second is even more challenging to our industry. How do we move our critical systems into the Cloud where we could, potentially, share infrastructure and technicians with other, non-critical businesses. And, how do we maintain physical security, cyber security, and reliability if we do so.

Now, and in the future, our industry is working with long-term vendors whose solutions, vital to the reliability and security of our operations, may no longer be supported as non-Cloud (i.e. on-site) solutions. This shift in services and supports available for our industry's critical functions will force our industry to shift focus as well. This shift is not limited to common desktop solutions; to the contrary, it includes some of the more high-tech security and operational solutions. We in the industry and our regulators must consider how regulatory requirements adapt to such a rapidly evolving set of changes and how we continue to innovate to enhance reliability, resilience and security in our systems.

#### **V. Current activity for enablement of Cloud Services**

The electric industry recognizes the need to look at how to enable Cloud computing -- a recent Standard Authorization Request (SAR) was submitted to NERC to provide high level guidance to update the NERC CIP standards. This is a critical first step in this industry's journey towards Cloud Services. Just last year I served as the chair of the CIP-008 Standard Drafting Team, working with a team of dedicated professionals to update the requirement to improve our cyber security incident reporting.

I am currently chairing the SAR drafting team working on modifications to two NERC CIP standards allowing us to begin storing BES Cyber System Information in the Cloud -- basically the first step towards Cloud enablement for our industry. As my team works through how to securely store and manage BES Cyber System Information we will pave the way for another group to look at how to move Energy Management Systems (EMS) and SCADA (Supervisory Controls and Data Acquisition) controls to the Cloud.

The theme I have developed for my drafting team as we consider Cloud Services is: Embrace it, Support it, Secure it. As an industry we should embrace Cloud Services because

they are here today, support Cloud Services because we need to work with our vendors as they move to Cloud Services, and secure Cloud Services because, just like our current IT services, our Cloud Services must be protected. Some in the industry refer to this information as our “crown jewels” or “keys to the kingdom.” We need to put protections in place to keep our most important assets secure.

## **VI. Conclusion**

There is no longer a question of “whether” Cloud Services have a place in our industry; today, there is a question of when, what, and how Cloud Services will work in our industry. Major software vendors have moved quickly from a “Cloud first” to a “Cloud only” mindset, and that tells us that older, non-Cloud technologies will not be supported indefinitely. Other aspects of Cloud Services (Software as a Service, Platform as a Service, and Infrastructure as a Service) are developing quickly.

The industry would benefit from focused attention by the Commission to advance the ability of companies to appropriately incorporate and leverage the economic and security benefits of Cloud computing. Changing and evolving technologies and innovations are outpacing the NERC CIP standards, creating a risk that the industry may not embrace these technologies and the enhancements to reliability, resilience and cyber security they offer. Current NERC standard development processes are not designed to meet such a rapidly changing environment.

We recommend the Commission further engage industry and key Cloud Services developers and providers in one or more technical conferences to first clarify issues and then, with that information, direct timely industry action to chart our way forward to enable appropriate CIP standards to accommodate the industry adoption of Cloud Services. This would

be consistent with the Commission's approach in other NERC CIP matters, including for example the recent modifications to CIP-008 incident reporting where a 6 month deadline was achieved. Cloud Services offer industry an opportunity to enhance security and reliability, and Commission leadership can help align best available Cloud Services, industry best practices and NERC and NERC CIP compliance. Such efforts will support future grid reliability and resilience for the benefit of all electricity customers.

We in the industry look to our regulators at the Commission and NERC to help us help our vendors provide Cloud Services that are reliable and secure, and that enhance our ability to keep the bulk electric system safe, reliable, resilient and secure.

Respectfully submitted,

*/s/ David Rosenthal*

David Rosenthal

Director, Incident Response & Systems Recovery  
for the Midcontinent Independent System Operator,  
Inc.

Dated: June 14<sup>th</sup>, 2019



## Appendix A

### **Panel II: The Impact of Cloud Based Services and Virtualization on BES Operations, Planning and Security**

- a. **Cloud Services providers offers many services to utilities from providing software as a service (SaaS) to infrastructure as a service (IaaS). How can Cloud Services be used effectively and securely for utility planning and operations? In what areas and what type(s) of applications? What, if any, use cases should not be considered for Cloud Services and why?**

Secure Cloud Services provides an array of capabilities in the areas of: reliability and resiliency, security and continuous monitoring, dynamic service right-sizing, big data analytics, as well as enhanced recovery capabilities. Cloud providers can provide better operational security than most organizations due in part to their advanced tools, processes, and capabilities that help them stay ahead of nations state/bad actor capabilities.

Regarding use cases that should not be considered today, placing any BES cyber system in the cloud poses additional risks and should be reviewed carefully to ensure the proper rigor and protection measures are applied.

- b. **What are the security and operational concerns associated with the increased use of virtualization in utility environments that must comply with the NERC CIP Reliability Standards? How can the NERC CIP Reliability Standards adapt to the increased use of virtualization?**

Many of the security and operational concerns around virtualization today are centered on both ensuring that the components of your visualization environment are well protected and monitored as well as managing the shared services aspect of the virtualization stack. Today many organizations already leverage virtualization in their ESP and have successfully passed CIP audits.

The shared infrastructure model provides additional risk from a performance and reliability perspective as well as a security perspective. When sharing virtualized infrastructure it is important to ensure that devices that are shared have the same risk profile and are separated such that less critical systems cannot affect the more critical systems. From an operational perspective, your OT systems can be affected by regular IT use and should never be mixed.

- c. Cloud based computing may be used for storage of information as well as performing non-real-time calculations, such as day-ahead planning studies. What real-time operations can leverage the flexibility of cloud based computing? What would that service look like from a usage and security perspective?**

Cloud based computing can potentially support a large number of workloads including real time services such as PowerFlow and state estimation. A cloud solution provides significant benefits to real-time workloads in the areas of availability, scaling and demand management.

- d. Discuss the potential security and operational benefits of Cloud Services and virtualized environments. For example, could the increased use of cloud and virtualized environments benefit operational planning and/or recovery and restoration processes?**

Cloud provides benefits from scale, resource sharing and automation. Private cloud still benefits from resource sharing and automation but trades off the scale for allowing a single organization to use and control the cloud in question. Cloud computing enables the following capabilities that impact operations:

- Deployment automation - Benefits resiliency and disaster recovery by providing the capability to recover a service or environment in minutes not hours.
- Auto Scaling Automation - Benefits resiliency by auto scaling application or system resources when additional resource is needed
- Automation also provides enhanced capabilities for compliance and control. This means that more opportunities exist to design and implement preventative and automated controls as opposed detective and manual due to the design of the technology (especially IaaS / PaaS).
- Automation also provides the opportunity to ensure consistency. As opposed to manual activities the automated actions can be more efficient with less chance of

error. This applies to operational activities with no compliance impact as well as those activities that are important and interesting to us all.

- Automation around actions such as deployments allows for repeatable testing
- Automation including testing allows for potentially minimizing risk by allowing for more frequent patching and updates (with automated testing that reduces errors and issues) as well as more frequent password changes.

Possible usage:

- Backup site – Backup to the backup or even a 4th site
- Location for massive scale business analytics (outside the control room for planning or Day-Ahead as an example)
- Location for software testing or training simulation that can be spun up and destroyed when not in use.

**e. How should the NERC CIP Reliability Standards be modified to help assist entities in addressing compliance concerns related to Cloud Services, while still encouraging the adoption of Cloud Services for appropriate planning and operations applications?**

Currently a Standard Authorization Request (SAR) was submitted to NERC, and upon approval NERC will standup a Standard Drafting Team to update the current CIP requirements allowing BES Cyber System Information to be stored in the cloud (project 2019-02 BES Cyber System Information Access Management). This will be the first step to enabling the industry to leverage the BES Cyber System Information stored securely in the cloud.

Regarding BES Cyber Systems in the cloud, we recommend the Commission further engage industry and key Cloud Services developers and providers in one or more technical conferences to first clarify issues and then, with that information, direct timely industry action to chart our way forward to enable appropriate CIP standards to accommodate the industry adoption of Cloud Services.

**f. Cloud-based resources can be used to process large amounts of information and perform complex computations. Please explain how the cloud can be used to support security such as analyzing security logs from firewalls, intrusion detection systems,**

**hosts, servers, and other systems since this type of data requires massive storage and processing. Discuss how virtualized security appliances, both on-site and in the cloud, may enhance the reliability of the grid.**

Cloud-based solutions provide the flexibility and value to store vast amounts of logs. By having a retention period of many months to a year or more we can identify anomalies that normally would not appear in more limited timeframes. Additionally, a number of different industry reports document dwell time for adversaries in an organization. In 2017 Mandiant reported dwell time in corporate environments was 99 days while others reported even longer with times of 191 days. Thus, the ability to leverage flexible storage options becomes important to ensuring the ability to trace back to a compromise's origin and identify root cause as well as all actions taken since the original event.

Analysis is enhanced with cloud-based systems by facilitating massively parallel computations. Enrichments, such as geotagging, to log events scale very well in this sense. The more computing power you can apply, the faster enrichments can be completed. This applies whether the resources are on-site or in the cloud. The flexibility to shift workloads allows organizations to take advantage of compute power. Analysis jobs that may run days can now be completed overnight or sooner.