

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

**Reliability Technical Conference )**

**Docket No. AD19-13**

**PREPARED STATEMENT OF ANTIWON JACOBS  
ON BEHALF OF THE AMERICAN PUBLIC POWER ASSOCIATION AND  
THE LARGE PUBLIC POWER COUNCIL**

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

**I. INTRODUCTION**

Thank you for the opportunity to speak to the Commission. My name is Antiwon Jacobs and I am the Director, Information Technology Security and Chief Information Security Officer for Sacramento Municipal Utility District (SMUD). These comments are submitted on behalf of the American Public Power Association (APPA) and the Large Public Power Council (LPPC).

APPA and LPPC support efforts to encourage the evaluation and potential adoption of cloud services and virtualization. APPA and LPPC believe that with FERC and NERC's support, registered entities will finally be afforded the opportunity to decide whether leveraging these technologies and services are appropriate for their own organizations.

Current NERC rules of procedure (ROP) and NERC Critical Infrastructure Protection (CIP) standards do not explicitly address the use of cloud services and virtualization, leaving the industry uncertain as to how to approach related security and compliance risks as they explore the use of these technologies. APPA and LPPC note that the use of virtualized technologies and cloud-based services continues to increase and recognize that with them comes a greater need to understand associated security risks and compliance obligations.

As a predicate for this discussion, I note that it is important that the electric industry, the entire NERC Enterprise and FERC recognize that while virtualization and cloud-services are related on the surface, the barriers to adoption of each are very different and distinct.

At the present date, many registered entities use Cloud Service Providers (CSPs) to manage a variety of business processes outside of power systems and power operations. However, the potential to use CSPs to support power delivery systems is upon us. The deployment of cloud technologies offers an opportunity for entities to increase visibility into system operations & security, improve system availability, and reduce resource requirements. If done with care and prudence, a technology and security architecture that incorporates cloud solutions can reduce risk, increase flexibility, and improve the security posture of the Bulk Electric Systems (BES).

I also want to strike a cautionary note: The use of a cloud-based technology to control energy management systems should not be considered at this time. In addition, the use of CSPs should not remove or circumvent critical layers of defense already in place to protect the BES.

## II. RESPONSE TO QUESTIONS

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?
Response:	<p>The deployment of cloud technologies offers an opportunity for utilities to increase visibility into system operations and security, improve system availability, and reduce resource requirements. If done with care and prudence, a technology and security architecture that incorporates cloud solutions can reduce risk, increase flexibility, and improve the security posture of the Bulk Electric Systems (BES).</p> <p>Cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) present different challenges to the management and control of cyber security risk and compliance risk. However, the different deployment models such as private cloud offers an opportunity for utility consumers to manage, and in some cases better control, cyber security risk associated with the confidentiality, integrity, and availability of data and technology in the cloud. FERC or NERC’s endorsement or acceptance of external accreditations such as the Federal Risk and Authorization Management Program (FedRAMP) could be leveraged to address compliance risk.</p> <p>Cloud architecture could empower utilities to effectively and securely introduce effective solutions that will allow for redeployment of resources to improve the security posture of the Bulk Electric System (BES). Focusing on cyber security planning and cyber security operations, cloud service models can improve cyber security control implementations for data protection (network and storage), monitoring, and compliance.</p> <p>Opportunities for the use of a CSP include:</p> <ul style="list-style-type: none"> <li>• Electronic Access Control or Monitoring Systems (EACMS)/ Physical Access Control Systems (PACS): CSP solutions present opportunities to deploy cost-effective advanced security tools to support NERC CIP EACMS and PACS security monitoring requirements and leading security practices. Specifically, CSP solutions for security event monitoring, intrusion detection, antivirus, endpoint disaster recovery, and multifactor</li> </ul>

	<p>authentication exist. These types of solutions enhance security operations and monitoring.</p> <ul style="list-style-type: none"> <li>○ Examples of industry leading cloud solutions for use case consideration include: IBM QRadar, Crowdstrike, SPLUNK, or other managed security monitoring services.</li> </ul> <ul style="list-style-type: none"> <li>● Bulk Electric System (BES) Cyber System Information (BCSI) and Compliance Monitoring and Assessment Processes: CSP solutions present opportunities to deploy information management programs (protect, store, and share), security governance oversight, and compliance tools to manage regulatory requirement obligations <ul style="list-style-type: none"> <li>○ Examples of industry leading cloud solutions for use case consideration include: ServiceNow (Governance, Risk, and Compliance, Asset Management, Change Management), Office 365 – SharePoint or AWS (BCSI access and sharing in a common data repository).</li> </ul> </li> </ul> <p>Use cases that <u>should not be</u> considered for cloud services at this time due to their greater inherent risk and impact are:</p> <ul style="list-style-type: none"> <li>● Services that can directly impact system reliability or control of energy management systems (e.g. Energy Management Systems (EMS) and SCADA (Supervisory Controls and Data Acquisition) controls).</li> <li>● Uses that might remove or circumvent critical layers of defense already in place to protect the bulk electric systems today. For example, critical layers of defense to PACS and EACMS such as operational security (physical), access points, authentication servers, and key management servers.</li> </ul>
<p>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?</p>	
<p>Response:</p>	<p>The NERC Project 2016-02 Standards Drafting Team has recently released a draft white paper titled Virtualization and Future Technologies. This white paper goes into extensive detail regarding virtualization, future technologies and specific examples of the need for revisions to the NERC CIP Reliability Standards.</p> <p>In line with NERC Project 2016-02, security and operational concerns associated with virtualization technologies are basically the same concerns associated with physical utility networked infrastructure that must comply with NERC CIP Reliability Standards. However, virtualization increases reliability and resiliency to control systems that support BES reliability. Virtualization technologies offer numerous benefits to reliability, scalability, fault tolerance, recoverability and security of the systems they run. Some of the key benefits of virtualization technologies are these:</p>

	<ul style="list-style-type: none"> <li>• Whole system backup and cloning, which allows an exact bit for bit copy of a virtual system to be made and kept in a warm standby state, ensuring rapid restoration if the primary virtual system fails.</li> <li>• Greatly streamlines recovery, as rebuilding a physical server is not required and instead the virtual systems can be moved to another system and accessed as normal. (Note: If cloud computing is factored in, then organizations do not need on-premise hardware to execute a restoration.)</li> <li>• Pooled raw computing resources, such as processors, memory and storage, allow for more efficient resource usage.</li> <li>• Flexible architecture, increased uptime, speedy recovery capabilities using dynamic resource management or orchestration software.</li> <li>• Zero-trust model architectures ensure no user or system is trusted by default from inside or outside the environment, and verification is required from any attempt to gain access to resources in the environment.</li> <li>• Micro-segmentation of virtualized systems provides security through the deployment of fine-grained security policies which are assigned to data center applications, down to the process level.</li> </ul> <p>The NERC CIP Reliability Standards could be modified to support the increased use of virtualization. Current NERC CIP Reliability standards do not address the concept of virtual infrastructure. The CIP Reliability standards will be most effective if they adopt a results-based approach.</p>
c.	<p>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?</p>
Response:	<p>Cloud-based computing presents opportunities to securely enhance the speed and collaboration activities with sharing BCSI or BES transmission data for internal reliability functions and external regulatory requirements. Cloud computing might also be leveraged to support the monitoring of operations, security and compliance. Regardless, FERC has an opportunity to establish precedent for cloud usage and security models to ensure utilities have a consistent and effective approach to addressing critical security requirements when considering a relationship with a CSP.</p> <p>I do want to emphasize that we may collectively enhance risk assurance through the use of external cloud accreditations and certifications like the Federal Risk and Authorization Management Program (FedRAMP) or System and Organization Controls (SOC) compliance. The scale of the resources a CSP can bring to bear on security, reliability, and risk reduction exceed that of most utilities, including the level of rigor and control monitoring. These can assist utilities with making decisions about different cloud deployment models to increase security and managing risk associated with the confidentiality, integrity, and availability of data and technology in the cloud.</p>

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?

Response: Some of the key security and operational benefits of cloud and virtualization technologies are these:

- Whole system backup and cloning, which allows an exact bit for bit copy of a virtual system to be made and kept in a warm stand by state, ensuring rapid restoration if the primary virtual system fails.
- Greatly streamlines recovery, as rebuilding a physical server is not required and instead the virtual systems can be moved to another system and accessed as normal. (Note: If cloud computing is factored in, then Organizations do not need on-premise hardware to execute a restoration.)
- Pooled raw computing resources, such as processors, memory and storage, allow for more efficient resource usage.
- Flexible architecture, increased uptime, speedy recovery capabilities using dynamic resource management or orchestration software.
- Zero-trust model architectures ensure no user or system is trusted by default from inside or outside the environment, and verification is required from any attempt to gain access to resources in the environment.
- Micro-segmentation of virtualized systems provides security through the deployment of fine-grained security policies which are assigned to data center applications at the process level.

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?

Response: Current NERC rules of procedure (ROP) and NERC Critical Infrastructure Protection (CIP) standards do not explicitly address the use of cloud services and virtualization. The standards do not specifically address compliance obligations related to the use of cloud services and virtualization, so industry is not clear how to approach the security and compliance risk as they explore the use of these technologies. APPA and LPPC recognize that the use of virtualized technologies and cloud-based services continues to increase, and with them comes a greater need to understand security risks and compliance obligations.

As we look at revisions to the standards, it is critically important that industry, NERC and FERC recognize that while virtualization and cloud-services are related on the surface, the barriers for adoption of each are very different and distinct.

The current NERC CIP Reliability Standards do not necessarily need to be modified to permit registered entities to use these technologies, although it would be most helpful for FERC, NERC and the industry to come to consensus on this point. This will provide regulatory certainty not present today for these technologies. For example, the NERC CIP standards do not necessarily have to be changed to address specific security controls like encryption, managing user

	<p>authentication and authorization, or permissions and password policies for say a SaaS storage solution.</p> <p>Utilities are responsible for compliance with NERC CIP Reliability standards and should exercise due care about data and application security decisions for higher performance, system availability, and cost savings for BES planning and operations. With this said, a signal or some form of endorsement from NERC and FERC that these services are permissible under existing standards would be useful.</p> <p>I note that security associated with the use of CSPs may be enhanced through the use of external cloud accreditations and certifications like the Federal Risk and Authorization Management Program (FedRAMP) or System and Organization Controls (SOC) compliance. These programs can assist utilities in making decisions about different cloud deployment models to increase security and manage risk associated with the confidentiality, integrity, and availability of data and technology in the cloud.</p> <p>Although NERC asked the CIP Committee Compliance Input Working Group (CIWG) to draft Implementation Guidance for the use of cloud, NERC has not published an official position on the acceptability of cloud usage. Since the June 2017 NERC Emerging Technologies roundtable, the CIWG researched the issue of demonstrating CIP compliance with CSPs. The CIWG determined that the use of a 3<sup>rd</sup> party auditing and certification process (e.g. FedRAMP Authorization) is the most reliable, secure and efficient approach to resolving issues with the adoption of cloud services. Unfortunately, the CIWG has neither the authority nor the ability to formally authorize Regional Entity auditing personnel to leverage suggested third-party auditing or certifications. The CIWG has provided their findings to NERC.</p> <p>I note that vendor accreditation has recently been recognized by NERC (Supply Chain Staff Paper) as a best practice, but more specific direction regarding the nature of such accreditation, appropriate standards and protocols is needed. Various industry groups and NERC are working on this matter, though assistance from the government in engaging vendors may be needed.</p>
f.	<p>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.</p>
Response:	<p>CSP solutions could offer the utility industry opportunities to leverage advanced cyber security technologies/tools and expertise to manage threats that could compromise the BES. Moreover, CSP solutions could address industry-identified lessons learned and noncompliance trends associated with administrative tasks</p>

	<p>such as log management, change management, and BCSI management. Focusing on cyber security planning and cyber security operations, cloud service models could improve cyber security control implementations for data protection (network and storage), monitoring, and compliance.</p> <p>Cloud services have the ability improve cyber security with offerings that focus on technical and administrative security controls for analyzing security logs from firewalls, intrusion detection systems, hosts, servers, and other systems.</p> <p>The deployment of cloud technologies offers an opportunity for utilities to increase visibility into system operations and security, improve system availability, and reduce resource requirements to maintain processes. If done with care and prudence, a technology and security architecture that incorporates cloud solutions can reduce risk, increase flexibility, and improve the security posture of the BES.</p>
--	--