UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Virtualization and Cloud Computing Services Docket No. RM20-8-000

Comments of the National Rural Electric Cooperative Association

The National Rural Electric Cooperative Association (NRECA) appreciates the opportunity to submit the following comments in response to the Commission's Notice of Inquiry in this docket.[1]

The Notice of Inquiry seeks comments "on the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system [BES] operations" and "on whether barriers exist in the Critical Infrastructure Protection (CIP) Reliability Standards, which are developed by the North American Electric Reliability Corporation (NERC) and approved by the Commission, that impede the voluntary adoption of virtualization or cloud computing services."[2] The Commission states that it "intends to use the record developed in this proceeding to determine whether it would be appropriate, pursuant to section 215(d)(5) of the Federal Power Act, to direct that NERC develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services by registered entities."[3] The Notice of Inquiry poses a series of questions grouped into four general topics:

[1] 170 FERC ¶ 61,110 (2020) (Notice of Inquiry).

[2] *Id.*, P 1.

[3] *Id.*, P 3. *See* 16 U.S.C. § 824o(d)(5) (2018).

- Scope of potential use of virtualization and cloud computing services
- Potential benefits and risks associated with virtualization and cloud computing services
- Potential impediments to adopting virtualization and cloud computing services
- Potential use of new and emerging technologies in the current CIP standards framework.[4]

NRECA appreciates the Commission's action to collect information on the potentials uses, benefits, and risks of virtualization and cloud computing services in the electric utility sector and to assess whether the CIP Reliability Standards accommodate these technologies while ensuring the reliability of the bulk power system. As described below, electric cooperatives use virtualization and cloud computing services because of the benefits they provide in flexibility, configurability, scalability, reliability, and resilience. Cooperatives recognize, however, that these technologies come with distinct risks, which must be accounted for in deciding whether and how to deploy these technologies and how to mitigate these risks. Cooperatives recognize that changes to the CIP Reliability Standards and the compliance and enforcement framework may help accommodate virtualization and cloud computing services while addressing their distinct risks. Cooperatives caution that such changes should be "backward compatible" and allow Registered Entities to continue non-virtualized, non-cloud operations and decide if, when, and how to use such technologies in BES operations and other services. NRECA's member cooperatives thus welcome the opportunity to comment on the questions posed in the Notice of Inquiry.

[4] *Id.*, P 14.

I. NRECA's Interest

The National Rural Electric Cooperative Association (NRECA) is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landmass.[5]

Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 63 generation and transmission (G&T) cooperatives and 834 distribution cooperatives. The G&T cooperatives generate and transmit power to distribution cooperatives that provide it to the end of line co-op consumer-members. Collectively, G&T cooperatives generate and transmit power to nearly 80 percent of the distribution cooperatives in the nation. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

NRECA's member cooperatives include Registered Entities subject to the Reliability Standards developed by NERC and approved by the Commission pursuant to section 215 of the Federal Power Act.[6] Nearly all cooperatives, even if they are not Registered Entities, receive service from the BES and thus have an interest in the

[5] See https://www.electric.coop/electric-cooperative-fact-sheet/

[6] 16 U.S.C. § 824o (2018).

reliability of the BES. Thus, NRECA's member cooperatives have significant interests in the topics of this inquiry.

II. Communications

Communications and service in this docket should be directed to the following persons:

Barry R. Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-5781
barry.lawson@nreca.coop

Randolph L. Elliott
McCarter & English, LLP
1301 K Street, NW, Suite 1000 West
Washington, DC 20005
(202) 753-3428
relliott@mccarter.com

III. Comments

A. Scope of Potential Use of Virtualization and Cloud Computing Services

In the Notice of Inquiry, the Commission states that virtualization and cloud computing services have "a wide variety of potential uses in the context of users, owners and operators of the bulk electric system" beyond simply cloud-based data storage, including potential uses for "BES reliability operating services."[7] Specifically, the Commission lists the following reliability operating services:[8]

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)

[7] Notice of Inquiry at P 16.

[8] *Id.*

- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

The first set of questions in the Notice of Inquiry concerns "the possible applications of virtualization and cloud computing services" in BES operations.[9]

A1. Identify and discuss which BES reliability operating services referenced above could be implemented in a virtualized environment.

NRECA's member cooperatives generally believe that all of these BES reliability operating services could be implemented in a virtualized environment. Indeed, some G&T cooperatives report that they have implemented all of the above services in a virtualized environment, and some have operated in a virtualized environment for years.

A2. Identify and discuss which BES reliability operating services referenced above could be implemented in a cloud computing environment.

NRECA's member cooperatives report that they have not implemented these BES reliability operating services in a cloud computing environment at this time and have security and other concerns about doing so. In general, cooperatives believe that the list of reliability operating services that could—or more properly—should be implemented in the cloud to be much smaller than those that can be implemented in a virtualized

[9] *Id.*, P 17.

environment.[10] While there may be advantages to implementing services such as state estimation and contingency analysis in the cloud, cooperatives generally do not believe that it is in their best interest at this time to implement critical real-time controls in the cloud, such as communication systems of last resort, blackstart capability, or dynamic response relays (due to the lag time from a cloud-based operation). In addition, it may be difficult for cooperative, especially in a rural area, to attract and retain skilled, trained, and certified staff to be cloud administrators or security personnel to work with a cloud services provider.

A3. Identify and discuss any other BES reliability operating or support services that could be implemented in a virtualized environment.

NRECA's member cooperatives generally believe that a number of other operating or support services could be implemented in a virtualized environment. This includes Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). In general, all server-based datacenter functions used to support the Industrial Control System (ICS) environment may benefit from the increased reliability, ease of deployment, scalability, configurability, and fast recovery afforded by a virtualized environment. Vendor support is a key deciding factor, however, because some vendors will not certify or support their applications in a virtual environment. This barrier is expected to decline over time.

[10] In this context, NRECA's members understand that "virtualization" generally means on-premise and managed by the utility or other Registered Entity, while "cloud computing" generally means off-premise and managed by a third party.

A4. Identify and discuss any other BES reliability operating, data storage or support services that could be implemented in a cloud computing environment.

Cooperatives generally believe that many of these other support services could be implemented in a cloud computing environment. Data storage is a common and well-understood use-case. Other uses for cloud-based services include many EACMS and PACS functions (such as PACS servers); Endpoint Detection and Response (EDR) tools, such as Microsoft Advanced Threat Protection; and security information and event management (SIEM) tools. Indeed, currently the most advanced EDR tools are almost exclusively offered via cloud computing environments. Cooperatives generally do not believe that network controllers should be implemented in a cloud computing environment at this time.

B. Potential Benefits and Risks Associated with Virtualization and Cloud Computing Services

In the second topic in the Notice of Inquiry, the Commission seeks comment on the potential benefits and risks associated with virtualization and cloud computing services.[11] NRECA members see both potential benefits and risks associated with virtualization and cloud computing services.

B1. What are the potential benefits associated with adopting virtualization for the BES reliability operating services identified in response to Questions A1 and A3?

Cooperatives have identified many potential benefits from virtualization of these BES reliability operating services:

[11] Notice of Inquiry at P 18.

- Increased reliability, with less hardware to fail, with multiple hosts permitting the migration of server clusters for higher availability and reduced or eliminated system outages; hypervisors themselves are redundant and guest failovers between sites can be done seamlessly; options for site failover.

- Faster disaster recovery, including recovery from hardware failures if properly configured; if a virtualized server fails a new one can be created in a much shorter time than it would take to procure a new physical server.

- Reduced hardware costs, because virtualized servers can be significantly less expensive that their hardware counterparts.

- Reduced hardware maintenance and operational costs due to the lower number of physical servers required.

- Reduced downtime on hardware maintenance by migrating virtual machines to other locations in the cluster.

- Higher hardware utilization.

- Easier management, including patch management.

- Improved agility from using virtualized servers; e.g., new instances can be spun up quickly to address capacity issues.

- Virtualized appliances provided by software vendors can dramatically reduce the time to implement new or enhanced features.

- Increased security due to physical access to a hypervisor versus physical security to multiple servers.

- Increased security with use of encryption.

- Zero Trust architecture is possible.

B2. Are there risks associated with adopting virtualization for the BES reliability operating services identified in response to Questions A1 and A3? If risks exist, discuss whether these risks can be effectively mitigated by a responsible entity.

Cooperatives have identified certain risks from adopting virtualization for the BES reliability operating services described in those questions. Shared resources or infrastructure may provide another attack surface. And fewer hardware components

(primarily hosts) may result in higher operational impact if a hypervisor or other primary components are compromised or fail.

Cooperatives nonetheless believe that many of these risks can be mitigated through proper training, network security, authentication security, and controls. Dedicated, redundant infrastructure for ICS environments, network segmentation, and applying principles of zero-trust to outside domains significantly reduces risk in these areas. Thus, one large G&T reports that it has not experienced any downside from adopting wide-scale virtualization. However, the cost and complexity of on-premise virtualization may be a barrier to smaller utilities with limited technical capabilities, leading them to explore managed cloud offerings instead.

B3. What are the potential benefits associated with adopting cloud computing services for the BES reliability operating services, data storage and support services identified in response to Questions A2 and A4?

NRECA's member cooperatives have noted several potential benefits from adopting cloud computing services for these BES reliability operating services, data storage, and support services:

- Cloud computing resources are more easily scalable to best fit the environment, allowing the entity to pay only for what is necessary and easily or rapidly expand capability based on demand.
- Some IT costs are outsourced for the backend infrastructure, which potentially may reduce the amount of in-house staff and labor costs associated with administrating local infrastructure.
- For the smaller utility with limited technical capabilities, the cloud potentially can provide improved security over what the utility might be able to have in a non-cloud environment.

- Increased reliability; major cloud providers provide redundancy across multiple datacenters, offering a level of resiliency that may not be possible to achieve with entity resources; options for site failover.

- Faster disaster recovery, including recovery from hardware failures if properly configured.

- No downtime for hardware maintenance.

- Easier management, including patch management.

- No physical access with the exception of the cloud provider.

- Increased security with use of encryption.

- Zero trust architecture may be possible in some cases but may entail higher costs from required additional equipment and expert in-house staff.

B4. Are there risks associated with adopting cloud computing services for the BES reliability operating services, data storage and support services identified in response to Questions A2 and A4? If risks exist, discuss whether these risks can be effectively mitigated by a responsible entity.

Cooperatives also have identified certain risks, particularly security risks, associated with adopting cloud computing services for the BES reliability operating services, data storage, and supporting services noted above. They recognize that certain measures can and should be taken to mitigate these risks.

Some of these risks are inherent in using an outside provider of cloud computing services. This potentially exposes an entity's network assets—normally in a closed network environment—to outside risks. Cloud resources themselves provide a more public-facing attack vector and additional access control considerations. Entities can reduce risk in this area by deploying cloud-environment specific monitoring tools and maintaining encryption keys or using secure encryption key technology provided by many cloud providers.

Another risk is the loss of control over, or even visibility into, the services being performed by the cloud provider or the problems that may arise on a cloud-based system that the cooperative does not own or control. This risk potentially can be mitigated, depending on cloud provider and what controls are implemented. Cloud-based systems are potentially less reliable because the cooperative is relying on a third-party's interpretation of what is adequate redundancy and security. A cooperative would depend on the cloud services provider to attest that it is doing the necessary patching, security monitoring, and overall threat mitigation on the provider's own system to keep the BES reliability operating services to which they have been entrusted reliable and secure. Auditing can mitigate these risks. But the cooperative would need a plan to switch cloud providers if the current one becomes unreliable.

When a cloud-based system goes down there is potentially increased outage time due to third-party administration and competition for remediation services. Moreover, in cloud-based, fee-for-service environments, larger users may receive a larger share of the attention and benefit from the provider.

A cloud-based system also relies on network connectivity. This increases the likelihood of connectivity loss, performance issues due to bandwidth, or increased latency, especially in rural areas. The severity of these issues can adversely affect real-time operation, and to a lesser degree monitoring systems. Redundant links with multiple internet providers and quality-of-service agreements can help mitigate these performance issues, but at an increased cost.

Appreciating these security and related risks, some cooperatives presently believe that cloud computing services should be reserved for limited purposes. Other

cooperatives believe that with the appropriate infrastructure and security measures in place, they could utilize the cloud at least as effectively as private infrastructure, if not more so given the other areas of benefit cloud services offer.

B5. What are the potential benefits of relying on third-party assessments to ensure the secure use of virtualization and cloud computing services for BES reliability operations and support services?

NRECA's member cooperatives have not reported extensive experience with third-party assessments for this purpose. However, they recognize there may be potential benefits. A third party may be well versed in new technologies and methodologies. A third-party assessment has the advantage of objectivity due to the fact that the assessor is someone who is not as close to the processes and can often view it more objectively. Using a third party may save time and simplify a registered entity's compliance auditing.

B6. Discuss any risks associated with relying on third party assessments to ensure the secure use of virtualization and cloud computing services for BES reliability operations and support services and potential solutions to mitigate those risks.

Once again, cooperatives have identified certain risks from relying on third-party assessments for this purpose, which require attention to certain mitigation measures.

A cooperative cannot be completely sure as to the qualifications and experience of the assessor. Among other things, a third-party assessment organization would need to understand the applicable standards. The solution would be to define which third-party assessment organizations meet the requirements.

Moreover, a third-party assessment organization may not fully understand a cooperative's virtual environment well enough to make an accurate assessment. The system would need to be fully documented to reduce this risk.

A related concern is that a utility's acceptance of a third-party assessment may not be acceptable to a NERC or regional auditor. This highlights the need for NERC and regional entity education. A third-party assessment organization also must protect the utility's data. This risk can be mitigated, at least in part, by appropriate contracts with the third-party assessment organization.

C. Potential Impediments to Adopting Virtualization and Cloud Computing Services

In the next section of the Notice of Inquiry, the Commission states that some participants in past Commission technical conferences asserted there was uncertainty about the treatment of virtualization and cloud-based services by the existing CIP reliability standards framework. Thus, the Commission "seeks comment on potential challenges with how the implementation of virtualization and cloud computing technologies will fit into the framework of the CIP Reliability Standards, and possible solutions to those challenges."[12]

C1. Provide comment on the validity of the panelists' concern discussed above and discuss the extent to which the trend toward cloud-based services could affect reliable and secure bulk electric system operations.

NRECA will address these issues in its responses to the questions below.

[1212] Notice of Inquiry at P 20.

C2. Are there any technical challenges in implementing virtualization technology for the BES reliability operating services identified in response to Question A1 that result from the current CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

As noted in the response to Question A1 above, G&T cooperatives currently use virtualized technology for some or all the BES reliability operating services referred to in that question. Nevertheless, cooperatives recognize that it is difficult for the CIP Reliability Standards to address all technologies and situations. As a consequence, some virtualization technologies are more easily implemented under current CIP Reliability Standards than are others.

For example, virtualized environments that do not share infrastructure and do not rely on dynamic provisioning of virtual machines present a one-to-one ratio of Cyber Assets for documentation in CIP-002 and technical Standards such as CIP-007 and CIP-010. On the other hand, virtualization technologies that use a "golden image" to dynamically build and teardown resources based on demand and use software defined networking (SDN) instead of typical hardware firewalls or switching infrastructure present challenges for meeting these requirements. In order to accommodate these architectures, the CIP Standards would need to clearly define what constitutes a Cyber Asset in this scenario and provide language to address access control technologies used by SDN that deviate from the conventional requirements of CIP-005 Electronic Security Perimeters and CIP-007 Ports and Services.

At the same time, the CIP Reliability Standards need to remain backward-compatible to allow Registered Entities to make their own decisions on whether and how to use virtualization and cloud computing environments to provide BES reliability

operating services. In other words, if the CIP standards are augmented, they should not become technologically prescriptive and should not negatively affect Registered Entities' existing implementation of non-virtualized or non-cloud BES reliability operating services or their existing CIP program implementation.

C3. Are there any challenges in implementing virtualization technology for the BES reliability operating services identified in response to Question A1 that result from compliance obligations associated with the CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

Please refer to the response to Question C2. The challenge may arise from the need for a Registered Entity to provide evidence to show how it is meeting the CIP Reliability Standards. Cooperatives generally believe the CIP Reliability Standards have done an acceptable job, up to this point, of allowing cooperatives to satisfy their compliance obligations via a virtualized environment. New uses of virtualized and cloud computing environments may present challenges to documenting compliance, as noted above.

C4. Are there any technical challenges in implementing cloud computing technology for the BES reliability operating services identified in response to Question A2 that result from the current CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

The technical hurdles in implementing cloud computing technology for these purposes are discussed in the responses to Questions B4 and C2 above. The overall challenge is to maintain a clear understanding of who is responsible for the elements of the system and at which levels.

For example, monitoring tools currently meeting the criteria for EACMS may not be permissible in a cloud-computing resource, because the current definition of BES Cyber Asset is potentially problematic when applied to a cloud-infrastructure environment. Modified Reliability Standards language separating "monitoring systems" from "access control systems," and allowing monitoring systems to function as BES Cyber System Information instead of a BES Cyber Asset would facilitate the use of advanced monitoring and security tools only available in a cloud-hosted environment.

C5. Are there any challenges in implementing cloud computing technology for the BES reliability operating services identified in response to Question A2 that result from compliance obligations associated with the CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

Please refer to the response to Question C4. In general, demonstrating compliance is more difficult with a cloud computing environment because the Registered Entity is relying on the cloud provider's servers. The Registered Entity is dependent on its cloud provider and the controls it has implemented, as well as the information placed in the cloud environment.

D. Potential Use of New and Emerging Technologies in the Current CIP Standards Framework

The Commission seeks comment on potential new and emerging technologies beyond virtualization and cloud computing that responsible entities may be interested in adopting for the BES reliability operating services and if the CIP Reliability Standards would allow these technologies to be adopted.

D1. In addition to virtualization and clouding computing, discuss whether the CIP Reliability Standards limit the ability to take full advantage of new and emerging technologies for BES reliability operating services. Explain the types of new technologies, the potential benefits and how the CIP Reliability Standards may limit their use.

NRECA does not have comments on these broader issues at this time.

Respectfully submitted,

/s/ Randolph Elliott

Jay Morrison
Vice President, Regulatory Affairs
Barry R. Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-5781
jay.morrison@nreca.coop
barry.lawson@nreca.coop

Sean T. Beeny
Randolph Elliott
McCarter & English, LLP
1301 K Street, NW, Suite 1000 West
Washington, DC 20005
(202) 753-3400
sbeeny@mccarter.com
relliott@mccarter.com

Counsel for National Rural Electric Cooperative Association

July 1, 2020