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

| | | |
|---|---|---|
| **Virtualization and Cloud Computing Services** | **)**<br>**)** | **Docket No. RM20-8-000** |

# COMMENTS OF THE ISO/RTO COUNCIL

Pursuant to the Federal Energy Regulatory Commission's ("Commission") Notice of Inquiry ("NOI") issued on February 20, 2020,[1] the ISO/RTO Council ("IRC")[2] submits these comments in response to the topics and questions posed by the Commission in the NOI.

In the NOI, the Commission seeks comments regarding the potential benefits and risks associated with the use of virtualization and cloud computing services, and whether barriers impeding the adoption of virtualization and cloud computing exist in the North American Electric Reliability Corporation, Inc. ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards.[3] Specifically, the Commission seeks comments on four primary topics: (A) scope of potential use of virtualization and cloud computing services; (B) potential benefits and risks associated with virtualization and cloud computing services; (C) potential impediments to adopting virtualization and cloud computing services; and (D) potential use of new and emerging

[1] Notice of Inquiry, *Virtualization and Cloud Computing Services*, Docket No. RM 20-8-000 (February 20, 2020).

[2] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"), California Independent System Operator ("CAISO"), Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator of Ontario, Inc. ("IESO"), ISO New England Inc. ("ISO-NE"), Midcontinent Independent System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and Southwest Power Pool, Inc. ("SPP").

[3] NOI at P 14.

technologies in the current CIP Reliability Standards framework.[4] The Commission also asks in the NOI whether it is appropriate for the Commission to direct action in order to facilitate the voluntary adoption of virtualization and cloud computing services.[5]

As more fully detailed below, the IRC believes virtualization and cloud computing services can be utilized for myriad reliability-related services, provided the risks are sufficiently mitigated through mandatory cloud security requirements, and that the Commission should direct action by NERC to develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services. Specifically, the existing CIP Reliability Standards need to be evaluated in light of cloud computing practices, and revised to address some of the nuances of cloud computing. This review should also consider the responsibility of the Registered Entity vis-a-vis the cloud service provider ("CSP"), and establish appropriate audit practices. The IRC stands ready to work with NERC, FERC, and the rest of the industry on this important task.

## I. COMMENTS ON TOPICS AND QUESTIONS IDENTIFIED IN THE NOI

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

The IRC believes cloud computing and/or virtualization technology can be used to implement each of the Bulk Electric System ("BES") reliability services referenced in the NOI: Dynamic Response to BES conditions; Balancing Load and Generation; Controlling Frequency (Real Power); Controlling Voltage (Reactive Power); Managing Constraints; Monitoring and Control; Restoration of BES; Situational Awareness; and Inter-Entity Real-Time Coordination and Communication. However, implementation of such complex, highly reliable services could pose

[4] NOI at P 14.

[5] NOI at P 13.

contractual and organizational challenges. This is because it would involve the re-implementation of technology and processes locally developed and highly refined over decades of effort within the industry, with the addition of new and different vendors and technical capabilities.

When considering the scope of virtualization and cloud computing services, the Commission should avoid limiting the discussion to virtualization of individual Cyber Assets. Virtualization should include the abstraction of more than the individual Cyber Assets to support newer approaches, like hyperconverged infrastructure and software-defined networking. Further, when considering virtualization, the scope should account for hybrid solutions that include both on-premises and cloud-based services to enable improved resilience.

Virtualization and cloud computing services should also be considered to enable advanced security measures, such as moving-target defenses, decoys, and zero-trust networking, which are not well-supported by the current CIP Reliability Standards. The scope should also discern the differences between on-premises cloud, single tenant cloud, and multi-tenant cloud solutions. The applicability, benefits, and security considerations may vary based on these different classifications. Moreover, the Commission should include in the scope software as a service, such as reliability functions provided completely as a service.

Technically speaking, any service that is implemented in a virtualized environment can be also deployed in a cloud computing environment. CSPs, such as Amazon, Microsoft, and Google, offer the Infrastructure-as-a-Service (IaaS) model on which the users are able to run virtual machines. These cloud-based virtual machines are like the on-premises virtual machines. They are hosted on physical servers in data centers with hypervisors running on the hardware or operating system level to logically isolate users. To guarantee the cyber security of virtual machines in the cloud environment, e.g., block unauthorized access, protect data at rest from being

breached, and data in-transit from being intercepted, users can deploy a complete set of IT rules on the cloud-hosted virtual machines ("VMs") the same as they define for their on-premises VMs and corporate network. If needed, users may even request dedicated-tenancy instead of shared-tenancy[6] for their VMs to further enhance the cloud security. When set-up diligently, the services implemented in a cloud environment can be as safe as in an on-premises virtualized environment.

It is essential though that all Reliability Standards that govern the deployment and operation of any BES reliability operating service in the cloud ensure the most stringent security controls and processes are applied. At no time should grid reliability functions be less secure than they would be in the most rigorous internally hosted environments. The CIP Reliability Standards must ensure the option to use cloud services only enhances and improves the overall security of the electric industry, and in no way diminishes what exists today.

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

Cloud computing must be implemented in a virtualized way, either through Paravirtualization ("PV") or Hardware Virtual Machine ("HVM").[7] Under either approach, the user lacks access to the physical server. Accordingly, IRC prefers to address this topic in two parts: Part A – what benefits and risks can virtualization bring (NOI Questions B1 and B2) and Part B – what additional benefits and risks can cloud services bring on top of virtualization (NOI Question B3 and B4)?

With virtualization, it is faster to provision the needed resources in terms of CPU, memory, storage, I/O per second ("IOPS"), and throughput. Some maintenance operations involving virtual

[6] Understanding AWS Tenancy. Available: https://theithollow.com/2017/10/16/understanding-aws-tenancy/

[7] CloudAcademy, "AMI Virtualization Types: HVM vs PV (Paravirtual VS Hardware VM)". Available: https://cloudacademy.com/blog/aws-ami-hvm-vs-pv-paravirtual-amazon/

systems may also be more efficient and reliable, such as operating system and application software updates or patches that may be implemented with the support of system snapshots (i.e. instant reversion to prior state should the update or patch fail for any reason). This assumes that much of the work is the delivery of the patch. However, in reality, the effort of patching is testing that does not change. Operating System ("OS") and hardware upgrades need to be tested whether located in the cloud or otherwise. IT workload could be reduced because security patches and software updates can be containerized for deployment. Virtualization also makes it easier to backup software applications that perform critical Bulk Electric System ("BES") reliability operating services and recover them from disasters. For this reason, virtual machines can achieve higher availability and robustness than physical servers, even in comparison to those with dual-server configurations. However, virtualization still has limitations. Not every application is going to work within a virtualized environment. For example, some legacy software tools require dongles and fail to support soft licensing mechanism. For on-premises virtualization, dynamic scalability requires investment in future capacity up front.

Cloud implementation shares most of the features of on-premises virtualization. The major factors to determine if a service should be implemented in the cloud computing environment or on-premises virtualized environment are mainly: (1) is system scalability needed; (2) does the service have high network usage; and (3) what are their respective costs?

Dynamic scalability is a challenge that on-premises virtualization may have when future capacity cannot be forecasted. Although business services grow as the power grid modernizes, the resources for computing, storage, and I/O via virtualization may not be able to become as large as

needed. By contrast, using cloud service facilitates both horizontal and vertical scaling.[8] The cloud provides theoretically unlimited access to resources upon request.[9] When there is a burst demand of cloud resources, for example, operation study to address time-constrained N-1-1 insecure problems,[10] the ability to scale up and down virtual machines is essential for the success of running these services virtually.

Network usage is another important point to decide which environment to adopt. If a service requires heavy inbound network traffic (assume the virtual machine takes a huge volume of data from an external source, for example, streaming PMU measurements for monitoring or control purpose), hosting it in a local virtualized environment could consume a large share of corporate network bandwidth based on design. Implementing this service in the cloud could avoid this situation by offloading this traffic to CSPs. Pay now or pay later corporate internal communication bandwidth is much cheaper than long distance communication. The inbound/outbound traffic goes through the internet gateways attached to a virtual private network on the cloud instead (e.g., Virtual Private Cloud in the context of Amazon Web Services (AWS) or Virtual Network in the context of Microsoft Azure). The IOPS and throughput of such a virtual network can be reconfigured with ease through some cloud service APIs.

Though not always determinative, cost considerations also inform whether on-premises virtualization or cloud services should be adopted. For on-premises virtualization, a large portion of the cost comes from the maintenance of the hosting physical servers that have to be always on. On the other hand, the cost of running BES services in the cloud can be minimized through the

[8] Horizontal scaling means adding more machines into the pool of resources whereas vertical scaling refers adding more power (CPU, RAM) to an existing machine.

[9] There could be administrative caps set by either the user's IT department or the CSP region limit

[10] X. Luo, S. Zhang, E. Litvinov, "Practical Design and Implementation of Cloud Computing for Power System Planning Studies," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2301-2311, Mar. 2019.

comprehensive and fine-grained pricing options offered by CSPs. Depending on business priorities, urgency, and objectives, users can choose to pay by time of use (spot instance), by fixed price regardless of actual time of use (on-demand instance), by long-term contract price (reserved instance), or by the number of invocations and resources allocation (service built on Function-as-a-Service model). For instance, when a Balancing Authority experiences an emergency SCADA or EMS loss, cloud services can be spun up to use PMU measurements on the tie-lines and key generators instead of lost SCADA to calculate Area Control Error ("ACE") and perform backup generation dispatch functionality. After the SCADA or EMS is back in service, the acquired cloud virtual resources can be returned to the CSPs because we no longer need them. In this case, using the least expensive event triggered Function-as-a-Service cloud computing model would be an ideal choice. However, such solutions need to be engineered and may have significant implementation and training costs associated.

When considering cloud security risks, it is important to recognize that cloud services have been compromised by advanced adversaries in the past. Most notably, Operation CloudHopper not only affected the cloud services, but also resulted in the infiltration of the customers' networks where integration existed with the cloud service providers.[11] When an unpatched vulnerability is identified by a CSP, it may have an impact on all of the tenants of that CSP, making the potential impact of a compromise much higher. As an example, a single critical vulnerability identified by researchers in the Azure environment could have allowed remote cloud execution if the researcher had not found the vulnerability and if Microsoft had not responded in a timely way.[12]

[11] https://insights.sei.cmu.edu/sei_blog/2019/03/operation-cloud-hopper-case-study.html

[12] https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/

Misconfiguration is also a commonly exploited vulnerability in cloud environments. A single misconfiguration may expose vulnerabilities on the internet, allowing the compromise of cloud infrastructure. Many cloud service customers have not fully developed their abilities to monitor for configuration changes in cloud services, so configuration drift may go unnoticed, extending the exposure time.[13]

In addition, although virtualization and cloud services should provide containment to prevent exposure of the hypervisor or other tenants, there are occasions when software vulnerabilities allow an adversary to escape from the containment and move laterally within the cloud infrastructure. This makes patch management a much more critical issue for cloud service providers.[14] Another risk of implementing cloud services is that customers do not typically understand and effectively apply the shared responsibility model. Customers may misplace their trust in the security offerings of the cloud service provider and fail to recognize the additional policies, processes, and technologies that need to be in place within the customer organization to fully secure the solution.[15] Moreover, privacy concerns exist. Any discussion involving data must address security and privacy, especially when it comes to managing sensitive data like CEII and dealing with CIP compliance. From this point of view, enforcing the same level of cyber-security compliance that would be used with on-premises servers is necessary. In addition to the common privacy concerns over nosy administrators, cloud services may not adequately protect data in the backup and clearing process, so customer data may become exposed through these means as well.

[13] https://www.ciodive.com/news/capital-one-breach-raises-questions-about-security-and-cloud-first-strategi/560129/

[14] https://eccitsolutions.com/security-hole-is-putting-many-containers-in-the-cloud-at-risk/

[15] https://eprints.usq.edu.au/33510/1/B5.%20Managing%20the%20Risks%20of%20Data%20Security%20and%20Privacy%20in%20the%20Cloud.pdf

Another risk of using cloud services is that differences between vendor platforms may create difficulties in migrating from one cloud platform to another. Gaps or compromises made during migration could also expose a user's data to additional security and privacy vulnerabilities. If a cloud service provider is acquired by foreign investors who are considered a risk to U.S. national security, vendor lock-in may prevent timely transition to a more secure vendor.[16]

Cloud-computing is also not without inherent risk from unplanned outages and interruption to services. For example, the Ashburn, Virginia AWS facility went black after losing power due to storms in June, 2012.[17] On Tuesday, February 28, 2017, an administrator's typo brought many websites and online applications to their knees.[18] A simple human error at Amazon S3, the backend for 150,714 websites, caused an outage. The S3 billing system had been acting sluggish, and associates were trying to debug it. One of them executed a command to remove a few servers from one of the subsystems that the S3 billing process used. With the errant stroke of a finger, the employee took out more servers than intended, causing collateral damage.

Another risk is a common mode failure and its associated risk to the BES. If multiple users in the same electrical interconnection or power region use the same cloud service, an outage of the cloud provider's facilities could have more severe consequences than if those users relied on different cloud providers. Some controls may be necessary to ensure sufficient diversity in cloud service providers.

[16] https://www.wsj.com/articles/u-s-officials-pressure-russia-linked-buyout-firm-to-sell-cybersecurity-company-11554925363

[17] https://www.pcworld.com/article/258627/amazon_cloud_hit_by_real_clouds_knocking_out_popular_sites_like_netflix_instagram.html

[18] https://www.networkworld.com/article/3178076/why-netflix-didnt-sink-when-amazon-s3-went-down.html

Internet availability remains the biggest risk to BES functions in the cloud. Today, real time operations can easily be islanded, and instructions to Transmission Owners, Generator Owners, or interties can be orchestrated through other communication modes like cellular or satellite phones. In case of a regional or larger internet connection failure, and assuming most of the BES functions are in the cloud, real time operators could potentially lose situational awareness.

Data sovereignty could be another potential risk. While access to BES-related data can be contractually restricted to entities within the United States and Canada, enforcement of that restriction or proof of access control may be hard to achieve. CSPs do perform zone transfers time-to-time that could potentially send BES data through other countries.

Finally, a significant risk of cloud services is the lack of customer visibility to vulnerabilities, cyber attacks, and compromises of the cloud service provider. Security practices must be considered that allow for monitoring and alerting to notify customers of attacks in progress. Customer incident response plans must also account for dealing with cyber attacks against cloud service providers.

**C. Potential Benefits and Risks Associated with Relying on Third-Party Assessments**

The IRC believes that the use of third-party assessments and certification would be beneficial and safely ease compliance burdens. By relying on reputable CSPs such as Amazon, Microsoft, and Google, Registered Entities can deploy their cyber systems to cloud service platforms that provide sophisticated protection against cyber threats and vulnerabilities, including anti-malware, web application firewall, intrusion detection systems, "Denial of Service" protection systems, and similar protections not provided at most on-site cyber facilities. These reputable CSPs have undergone rigorous audit and certification processes including FedRAMP and SOL certification. The federal government develops and manages FedRAMP as a government-wide

program providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud services; therefore, relying on CSPs that have FedRAMP certification can be trusted for the secure use of the cloud computing services.

As for physical security, CSPs are all required to build their data centers according to ISO 27001 requirements. These data centers are typically housed in nondescript facilities. CSPs physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. They use two-factor authentication, biometric-controlled locks, video surveillance, and regular access reviews to ensure the physical integrity of their servers. Generally, the physical security of the cloud data center is higher than that of utilities and ISOs.

To address potential personnel risks, reputable CSPs often offer a government cloud service (for example, AWS GovCloud or Azure Government). The government cloud requires a higher security clearance, US citizenship, and separate account ID and user access credentials in additional to the standard cloud services.

**D. Potential Impediments to Adopting Virtualization and Cloud Computing Services**

To date, many Registered Entities see the current regulatory framework as prohibiting the adoption of cloud computing resources in support of BES reliability functions or monitoring. Many utilities have not fully deployed virtualization technologies because they feel they would be increasing their compliance risk. There are several efforts underway with NERC Standards Drafting Teams to address some of those provisions. Until those efforts have been completed and standards have been changed, many utilities will not move forward to take full advantage of the

benefits of virtualization or cloud computing technologies in support of the reliability functions noted in the NOI.

While it is technically possible in principle to implement BES reliability operating services via cloud computing, there may be contractual and business challenges associated with specific software application or library dependencies, runtime environments or licensing restrictions related to virtualization as used in a cloud environment—for example, as pointed out above, when soft licensing mechanism is not supported. Nevertheless, with additional industry adoption, software vendors will have a greater incentive to adopt suitable licensing agreements.[19]

The major concerns and impediments are the compliance risks, especially with respect to the CIP Reliability Standards. Ultimately, it is the Registered Entity's responsibility to ensure CIP compliance. Failure to comply with CIP Reliability Standards may result in significant penalties. NERC has not addressed yet whether and how Registered Entities may pass a CIP Standards audit with workloads hosted in the cloud. As a result, Registered Entities face significant uncertainty and an auditor may disagree with the Registered Entity's approach to cloud deployment.

From the cloud providers' perspective, both AWS and Microsoft Azure have released official user guides to support compliance with the current version of the CIP Reliability Standards, indicating that each CIP requirement can be strictly met by enforcing security rules through various cloud services.[20] Noting that the major CSPs offer state-of-the-art updates on Information and

[19] Microsoft Azure, "Shared responsibility in the cloud". Available: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

[20] Amazon Web Services, "AWS User Guide to Support Compliance with NERC CIP Standards". Available: https://d1.awsstatic.com/whitepapers/aws-support-compliance-nerc-cip-standards.pdf?did=wp_card&trk=wp_card; Microsoft Azure, "Cloud Implementation Guide for NERC Audits", Available: https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=68df41b2-873d-4e4b-a7c8-8a0d4fdefb88&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_Compliance_Guides

Communications Technology (ICT), some services provide even more stringent protection than the CIP Reliability Standards require. For instance, CIP-012, which is yet to be implemented, deals with communications between control centers.[21] Applying it to the case of real-time PMU data, for example, CIP-012 would mandate using Internet Protocol Security (IPSec)-based VPN with AES-128 encryption. While AWS enables users to connect to their VPCs through IPSec-based site-to-site VPN with additional AES-256 encryption, a stronger encryption algorithm exists.[22] A requirement for the use of a specific technology is a poor choice for standard development.

It is infeasible for a CSP to accommodate audits initiated by individual NERC Registered Entities. We strongly suggest NERC explicitly endorse certifications performed by reputable U.S.-based auditing companies that are based on control evidence, assuring that controls are equivalent to those required under applicable CIP Reliability Standards and have been examined and approved through rigorous auditing processes. Certification could provide a more efficient approach to addressing NERC audit requirements.

The current CIP Reliability Standards were developed with physical systems in mind, requiring Registered Entities to identify BES Cyber Assets, group them into BES cyber systems, place them inside an electronic security perimeter, and place everything inside a physical security perimeter. With cloud computing services, virtual machines could be used when needed and returned to CSPs when the required tasks are finished. A Registered Entity, by contrast, cannot easily identify all the hardware used in the cloud environment, determine which of the cloud

[21] CIP-012-1, "Cyber Security – Communications Between Control Centers". Available: https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-012-1&title=Cyber%20Security%20–%20Communications%20between%20Control%20Centers&jurisdiction=United%20States

[22] Amazon Web Services, "Site-to-Site VPN Categories". Available: https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-categories.html

systems should be considered BES Cyber System, or protect the cloud hardware inside an Electronic Security Perimeter. For this reason, it is difficult to understand how an ESP would exist in a CSP's environment.

Virtualization and cloud computing services have matured for more than a decade. We encourage the Commission to direct NERC to develop forward-looking, technology-agnostic standards so that new and emerging technologies that are beneficial to the Registered Entities can be adopted to make BES reliability operating services more secure, efficient and reliable.

**E. Commission Action**

The IRC suggests that the Commission consider five actions in order to facilitate the voluntary adoption of virtualization and cloud computing services.

First, the IRC recommends the Commission direct NERC to work with industry to define security practices that sufficiently address the potential risks of cloud services. These security practices should be used as the basis for Reliability Standards that define the Responsible Entity's requirements when cloud services are used for reliability functions or BES Cyber System Information.

Second, the IRC suggests that the Commission direct NERC to modify its Compliance Monitoring Enforcement Program ("CMEP") and Reliability Standards (or accompanying compliance measures) in order to allow FedRAMP or comparable certifications as an acceptable means of demonstrating compliance with CIP Reliability Standards with respect to the utilization of cloud computing services. Current auditing requirements and Reliability Standards do not allow auditors or Registered Entities to rely on third-party certifications for purposes of determining and demonstrating compliance. Instead, overly-prescriptive compliance obligations may discourage the voluntary adoption of emerging technologies. Third-party certification could ease the

compliance burdens on Registered Entities and thereby encourage the use of emerging technologies, like cloud computing services. Acceptance of third-party certification could also ease the burden on CMEP auditors by allowing them to rely on third-party subject matter experts rather than having to independently verify compliance.

Third, the IRC suggests the Commission direct accelerated timelines for certain existing CIP Reliability Standard projects. Specifically, the IRC believes development is proceeding too slowly and requests that the Commission accelerate these projects and identify completion deadlines for Project 2016-02: Modifications to CIP Standards and Project 2019-02: BES Cyber System Information Access Management, with ample time provided for implementation and coordination on compliance guidance with NERC following Commission approval of resulting Reliability Standards. An accelerated approach for CIP Reliability Standard development has been successful and beneficial in the past. For example, the Commission issued its Order on Reliability Standards for Physical Security Measures under Docket No. RD14-6-000 on March 7, 2014, in which it directed NERC to file proposed Reliability Standards within 90 days of the date of the order. That Order resulted in the filing of CIP-014-1: Physical Security on an abbreviated timeline. While 90 days is likely more acceleration than is necessary for Project 2016-02: Modifications to CIP Standards and Project 2019-02: BES Cyber System Information Access Management, the IRC believes these projects should move more rapidly.

Fourth, the IRC suggests that the Commission direct that the NERC Standards Processes Manual (Appendix 3A to the NERC Rules of Procedure) be revised to permit abbreviated standard drafting processes if needed, when more reliable and secure technology becomes available. A more agile development process for emerging technologies could result in the earlier adoption of more beneficial and cost-effective practices. Accelerated drafting timelines are not readily

available under the current Reliability Standard development framework and would be beneficial, provided that registered entities are offered adequate time to review and comment on standards at NERC, and that implementation periods following Commission approval are sufficient to permit orderly technology and process changes where needed.

Finally, the IRC suggests that the Commission encourage NERC to consider more discrete Reliability Standard revisions where appropriate for emerging technologies, as opposed to broadly modifying existing Reliability Standards that were developed prior to and without regard to new technologies. This approach may result in a more efficient Reliability Standard development process to address the specific complexity of emerging technologies, allow earlier use of these technologies, and allow the earlier adoption of Reliability Standards that more clearly accommodate new technologies. It may also more quickly eliminate potential compliance uncertainty that exists in attempting to interpret how new technologies fall within preexisting Reliability Standards that may not be a natural fit. This approach could also reduce confusion for entities that do not plan to use these new technologies. Conversely, the IRC also believes that the National Institute of Standards and Technologies ("NIST") Cybersecurity Framework may provide an alternative compliance approach that would more easily allow the use of emerging technologies. Moreover, a results-based compliance approach, as opposed to a control-based approach, may also encourage the use of emerging technologies and/or hybrid approaches involving emerging technologies.

## II. CONCLUSION

The IRC respectfully requests that the Commission consider its comments on the topics and questions identified in the NOI.

Respectfully submitted,

*/s/ James M. Burlew*
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
**PJM Interconnection, L.L.C.**
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

*/s/ Margoth Caley*
Maria Gulluni
Vice President & General Counsel
Margoth Caley
Senior Regulatory Counsel
**ISO New England Inc.**
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

*/s/ Anna McKenna*
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
Andrew Ulmer Director, Federal Regulatory Affairs
**California Independent System Operator Corporation**
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

*/s/ Carl F. Patka*
Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Carl F. Patka
Assistant General Counsel
Christopher R. Sharp
Senior Compliance Attorney
**New York Independent System Operator, Inc.**
10 Krey Boulevard
Rensselaer, NY 12144
cpatka@nyiso.com

*/s/ Andre T. Porter*
Andre T. Porter
Vice President, General Counsel & Secretary
Mary-James Young
Senior Corporate Counsel
**Midcontinent Independent System Operator, Inc.**
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

*/s/ Paul Suskie*
Paul Suskie
Executive Vice President & General Counsel
Mike Riley
Associate General Counsel
**Southwest Power Pool, Inc.**
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

*/s/ Devon Huber*
Devon Huber
Senior Manager, Regulatory Affairs
**Independent Electricity System Operator**
1600-120 Adelaide Street West
Toronto Ontario M5H1T1
Canada
devon.huber@ieso.ca

*/s/ Chad V. Seely*
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
**Electric Reliability Council of Texas, Inc.**
7620 Metro Center Drive
Austin, Texas 78744
chad.seely@ercot.com

*/s/ Diana Wilson*
Diana Wilson
Director Enterprise Risk Management and Compliance
**Alberta Electric System Operator**
#2500, 330 – 5 Avenue SW
Calgary, Alberta T2P 0L4
diana.wilson@aeso.ca

July 1, 2020

Document Content(s)