UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION REGARDING BULK ELECTRIC SYSTEM OPERATIONS IN THE CLOUD

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

December 17, 2021

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION REGARDING BULK ELECTRIC SYSTEM OPERATIONS IN THE CLOUD

Pursuant to paragraph 17 of the Order Directing Informational Filing,[1] the North American Electric Reliability Corporation ("NERC")[2] hereby submits to the Federal Energy Regulatory Commission ("FERC" or the "Commission") an informational filing regarding Bulk Electric System ("BES") operations in the cloud.[3] Specifically, this informational filing (1) addresses the status of NERC's formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner, (2) evaluates potential modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards to facilitate expanded use of the cloud, and (3) considers topic areas raised in comments to the Notice of Inquiry ("NOI")[4] issued in the above captioned docket.

As noted in its comments in response to the NOI, NERC recognizes the benefits of cloud computing services and supports registered entities' use of cloud services as long as they use appropriate security measures to mitigate risk and maintain compliance with applicable Reliability Standards. In particular, one such benefit includes entities' gaining efficiencies to help ensure

---

1 *Virtualization and Cloud Computing Services*, Order Directing Informational Filing, 173 FERC ¶ 61,243 (2020) [hereinafter December 2020 Order].

2 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

3 Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, https://www.nerc.com/files/Glossary_of_Terms.pdf.

4 *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 (2020).

reliable service for customers of the Bulk-Power System ("BPS"). Additionally, NERC recognizes that technology evolves rapidly, and industry needs to be prepared to deploy these evolving technologies in a secure and reliable manner. Moreover, NERC is aware that registered entities have securely leveraged cloud computing services to host activities that are outside the purview of CIP compliance (e.g., reliability studies, forecasting, etc.).

To that end, NERC acknowledges that continued assessment of the feasibility and security of BES reliability operating services[5] in the cloud is both appropriate and necessary. While the CIP standards do not expressly prohibit BES reliability operating services in the cloud, a standards development project may be initiated in the future to revise the CIP standards to better accommodate certain cloud security features. In the meantime, additional analysis is necessary to understand the types of controls that would allow industry to realize the potential reliability benefits of hosting BES reliability operating services in the cloud while mitigating known security risks. In the coming years, NERC, in collaboration with the Reliability and Security Technical Committee ("RSTC"), will help support entities in progressing toward securely using the cloud for BES reliability operating services.

This informational filing is organized as follows: Section I is background describing the NOI and December 2020 Order. Section II provides the NERC process to assess the feasibility of BES reliability operating services in the cloud. Section III outlines some considerations for CIP standards development activities to accommodate the use of cloud services. Section IV discusses

[5] The Commission referenced the following BES reliability operating services: (1) Dynamic Response to BES conditions, (2) Balancing Load and Generation, (3) Controlling Frequency (Real Power), (4) Controlling Voltage (Reactive Power), (5) Managing Constraints, (6) Monitoring & Control, (7) Restoration of BES, (8) Situational Awareness, and (9) Inter-Entity Real-time Coordination and Communication. These are included in the non-enforceable Guidelines and Technical Basis section of CIP-002-5.1a at pages 17-18.

the topic areas from the NOI comments as directed in the December 2020 Order. Finally, Section V provides a conclusion to this informational filing.

I. BACKGROUND

On February 20, 2020, the Commission issued a NOI seeking comments regarding the use of virtualization[6] and cloud computing services[7] in association with BES operations, particularly in reference to the BES reliability operating services. The Commission recognized the evolving and increasing use of these technologies, particularly by vendors providing services to registered entities, and issued the NOI to understand how the Commission may support registered entities that are considering using these technologies in their real-time operating environments.

In response to comments received, the Commission issued the December 2020 Order directing NERC to: (1) begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner; and (2) make an informational filing that evaluates potential modifications to the CIP Reliability Standards to facilitate expanded use of the cloud, including performing BES operations. Specifically, the Commission stated that the informational filing should report on any new or future NERC standard drafting projects, including their status and schedule, and consider the comments received in response to the NOI regarding the following topic areas:

1. Ensuring quality of service and resilience;

---

[6] "Virtualization is the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical hardware resources required to perform various functions." NOI at P 4 (citing the National Institute of Standards and Technology ("NIST"), *Guide to Security for Full Virtualization Technologies*, Special Publication 800-125 (Jan. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.).

[7] The NIST Information Technology Laboratory Computer Security Resource Center defines cloud computing as a "model for enabling 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." NOI at P 7 (quoting NIST, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.).

2. Compliance oversight;
3. The potential benefits and risks associated with the use of virtualization and cloud computing services in association with BES operations, including the security objectives to mitigate risks by registered entities voluntarily using virtualization implemented off-premises and cloud computing;
4. The potential for the use of BES reliability operating services data and the storage or use of BES Cyber System Information ("BCSI") outside the registered entity's country;
5. Evaluation criteria for the selection of cloud service providers for use by the electric industry;
6. Allowing registered entities to conduct their own reliability risk assessments to determine what BES reliability operating services and other services can be securely performed in the cloud;
7. Establishing a clear dividing line between the security responsibilities of the cloud service provider and the registered entity; and
8. Whether to establish a new audit process, which could provide auditors access to cloud service providers' facilities.

The Commission directed that this informational filing be submitted by January 1, 2022.

II. PROCESS TO ASSESS FEASIBILITY OF CONDUCTING OPERATIONS IN THE CLOUD

Consistent with the directive in paragraph 17 of the December 2020 Order, NERC initiated a formal process to assess the feasibility of voluntarily conducting BES reliability operating services in the cloud in a secure manner. NERC developed the following steps as part of its process: (1) engage industry through the recently-established Security Integration and Technology Enablement Subcommittee ("SITES") of the NERC RSTC; (2) engage with cloud service providers; (3) discuss each topic area from the NOI with industry, cloud service providers, and Electric Reliability Organization ("ERO") Enterprise staff;[8] (4) consider whether a field test is needed;[9] (5) evaluate whether Reliability Standards revisions should be pursued; and (5) initiate

[8] The ERO Enterprise collectively refers to NERC and the six Regional Entities.

[9] Under section 6.0 of the Standard Processes Manual (Appendix 3A to the NERC Rules of Procedure), a drafting team (either a SAR or standards drafting team) may initiate a field test to test a concept before developing requirements. However, this means that a SAR must have been submitted and accepted to initiate a field test. Given there is not a SAR at this time, a field test cannot be conducted.

Reliability Standards development projects, if necessary. Given the importance of mitigating any risks of conducting BES reliability operating services in the cloud, NERC determined a deliberate, intentional approach necessary to appropriately move forward.

Currently, NERC has initiated the first three steps of its process. NERC will continue to engage with industry, cloud service providers, and ERO Enterprise staff to further explore how to address risks of BES reliability operating services in the cloud. In addition, SITES members plan to produce a whitepaper that outlines their input on these risks. The SITES and Security Working Group under the NERC RSTC are best suited to develop an industry position on this topic and pursue appropriate use of the cloud (through the development of Standard Authorization Requests ("SARs")) to move this topic forward if and when appropriate. These industry groups are well-positioned to gather feedback from industry on interest in using cloud computing services for BES reliability operating services, and NERC commits to collaborating with stakeholders to help ensure a coordinated approach to working towards solutions as necessary

III. POTENTIAL CIP STANDARDS MODIFICATIONS

NERC recognizes there may be need for revisions to the CIP Reliability Standards to facilitate registered entities' use of cloud computing technology for the BES reliability operating services. While the CIP standards do not explicitly prohibit use of cloud computing services, the standards were not drafted to account for certain security features of the cloud and may require modification for registered entities to implement these security features. Following the completion of assessment activities and other technical committee work, the following, non-exhaustive list of issues, among others, may need to be considered in CIP standards development activities:

- Revision to the "perimeter" security model (i.e. Electronic Security Perimeter with Electronic Access Point). Project 2016-02 is currently revising the CIP Reliability Standards to permit more "zero trust" models in addition to the traditional firewall-

based network model. These revisions will likely further enable cloud use because "zero trust" principles can be useful in cloud computing, but there likely will need to be more cloud-centric revisions after Project 2016-02 completes its work on virtualization.

- Revisions to how physical devices and their locations are handled. Project 2016-02 is currently revising definitions and certain physical access requirements to reflect virtualized technologies. These definitions and requirements are likely to need further clarification if registered entities are to rely on a third-party when it is located in a different country than the entity; there would also be considerations about the potential for sharing the underlay[10] resources with other tenants in a cloud service provider's environment.
- Consideration of impacts to any current definitions. For example, the Control Center definition, which currently includes "associated data centers," may be impacted by any standards development that accommodates cloud services. If third parties manage the data center of a Control Center that is using BES reliability operating services in the cloud, any standards development project would need to consider how to address the security controls that the existing CIP Reliability Standards direct for data centers.
- Consideration of objective-based requirements. The December 2020 Order directed NERC to consider whether requirements focused on security objectives would be appropriate. NERC would be supportive of objective-based requirements should industry indicate support through consensus.

[10] In a cloud environment, the underlay includes those resources, such as the communication gear, servers, or applications, managed by the cloud service provider.

The standards development process is open and inclusive consensus-building, and stakeholders may identify other issues for consideration in addition to the issues identified above. Further, stakeholders may ultimately determine that they do not wish to pursue adoption of these technologies absent a demonstrated reliability or security need. As of the date of this report, NERC has not received any SAR to initiate revisions to facilitate BES reliability operating services in the cloud.

Moreover, at this time, NERC has not identified a reliability gap that would necessitate Reliability Standards requirements that further facilitate BES reliability operating services in the cloud. Therefore, aside from the revisions identified above in Project 2016-02, NERC does not have any current or future projects planned to revise the Reliability Standards to further enable BES reliability operating services in the cloud. NERC can continue to pursue other activities to support registered entities' use of cloud computing services but will not revise the CIP standards until a SAR initiates a project. Such activities include collaboration with the RSTC on comprehensively addressing how to mitigate the security risks when moving aspects of the BES reliability operating services into the cloud environment, among others.

On a related note, NERC recently filed for Commission approval Reliability Standards CIP-004-7 and CIP-011-3.[11] The Commission approved these standards on December 7, 2021 via a delegated letter order.[12] The revisions in these Reliability Standards provide increased options for registered entities to leverage third-party data storage and analysis systems in a secure manner

[11] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards CIP-004-7 and CIP-011-3 Addressing Bulk Electric System Cyber System Information Access Management*, Docket No. RD21-6-000, (Sep. 15, 2021).

[12] FERC, *Petition of the North American Electric Reliability Corporation for Approval of Reliability Standards CIP-004-7 and CIP-011-3*, Letter Order, Docket No. RD21-6-000 (December 7, 2021).

for BES Cyber System Information ("BCSI"). As entities begin to implement these standards,[13] NERC will review how registered entities use cloud computing services for BCSI to inform NERC's assessment of the use of cloud computing services for BES reliability operating services.

IV. CONSIDERATION OF NOI COMMENTS

As directed in the December 2020 Order, NERC further considered the topic areas identified in the comments in response to the NOI. When considering these topic areas, NERC consulted with industry stakeholders, cloud service providers, and ERO Enterprise staff to determine how they could impact Reliability Standards development and compliance monitoring activities. The feedback and input provided during these discussions are incorporated in NERC's considerations of the topic areas below. The following subsections address the topic areas from the December 2020 Order.

A. Quality of Service and Resilience

As stated in the ERO Enterprise comments in response to the NOI, NERC acknowledges the benefits that cloud technology could provide in terms of quality of service[14] and resilience, as long as sufficient security controls, redundancies, failovers, and backup systems are in place to support BPS reliability. During discussions with industry stakeholders, registered entities agreed that quality of service and resilience need to be maintained at adequate levels to support BES reliability operating services in the cloud. In turn, the cloud environment could provide shared resources to a network that support a level of quality of service and resilience that would be difficult to achieve otherwise. Nevertheless, the same shared resources could pose problems for BES reliability operating services, particularly because high levels of quality of service are critical

[13] Pursuant to the implementation plan for CIP-004-7 and CIP-011-3, registered entities may elect to adopt these Reliability Standards provisions prior to the standards' effective date to facilitate use of cloud computing services for BCSI storage.

[14] Quality of service is the performance, availability, and reliability offered by the cloud service provider.

for real-time systems performing the BES reliability operating services functions. Thus, registered entities must ensure certain levels of quality of service and resilience are maintained, including by telecommunication providers, prior to engaging cloud service providers to host BES reliability operating services functions.

Systems performing the BES reliability operating services functions, and the applications contained within those systems, depend on high precision measurements, very high data availability, and low latency. Data points throughout the system are aggregated and used by the applications, systems, and tools that perform the functions essential to BPS reliability, ranging from situational awareness, state estimation, and contingency analysis tools to critical remedial action schemes that must operate within strict time limits. Data availability and integrity are absolutely critical for these systems; latency or unavailable data pose significant risks to these time-sensitive functions. In fact, during preparation of this informational filing, one cloud service provider experienced an underlay outage that impacted tenants' ability to operate and access their environments. Before moving any time-sensitive functions to the cloud, registered entities would need to consider ways to mitigate the risk of such an outage. In addition, BES reliability operating services functions rely on the availability and integrity from telecommunication providers.

A related consideration is the telecommunication paths that are used to transfer data. When those paths are owned by the registered entity, there is likely to be extremely low latency and high availability. However, prescribing a similar requirement in a service level agreement with a cloud service provider would mean the registered entity must evaluate how critical functions would be affected by data that must traverse a more complex telecommunication path that includes the cloud environment as well as field devices that control physical assets.

Moreover, the context of the BES reliability operating services functions to be performed is a key factor when determining what "quality of service" is required in a cloud environment. For example, a network architecture that includes system components that communicate with a third-party cloud service provider could also present an increased attack surface that results from added processes (e.g., converting serial to IP-based protocols). Any increased risk could also lead to increased compliance obligations and could introduce unacceptable latencies. Further, routing all system measurements to a third-party cloud service provider could degrade existing redundancies in the system and thereby eliminate or significantly degrade any benefit of cloud technology.

Similarly, cloud technology also presents benefits to data resilience within the cloud environment. While the cloud provides the capability to leverage multiple cloud regions, locations, or data centers with seamless failovers, resilience (like quality of service) must be considered from the perspective of the entire network architecture and not be limited to the cloud service provider environment alone. Communications networks connect field devices to the control center environment, to the cloud service provider environment, and possibly others. When making decisions about resilience matters, each network path needs to be considered, especially since control center applications use (and require) data from neighboring systems and that data must be aggregated before being passed to the cloud environment.

Each step is a potential point of failure (i.e., outage of the communications path) that needs to be mitigated to ensure that data is completely and securely moved while it is within the registered entity's direct control (e.g., control center, devices, etc.), while it is using the services of the telecommunication provider, and while it is processed by the cloud service provider. In all cases, however, overall responsibility for developing and maintaining a resilient system does not

move to the cloud service provider or the telecommunication provider; it remains with the registered entity operating BES reliability operating services in the cloud.

B. Data Residency

Data residency refers to "the requirement that all customer content processed and stored in an IT system remain within a specific country's borders."[15] This topic area is particularly a focus of governments seeking to protect data from other countries' requests when using multinational cloud service providers. While cloud service providers argue that strict data residency requirements limit data resilience and actually can hinder data security, they also acknowledge that there are circumstances when the location for certain highly sensitive or critical information may need to be restricted to specific zones or countries.

Cloud service providers have stated that they can allow customers to control where data will physically reside within the cloud service providers' data centers. For example, customers can select the regions or areas where their data will be stored, and the cloud service provider will not move that data without the customer's consent or request. In such instances, data is not moved unless it is built into a custom design, as specified by the customer. Therefore, data can be configured to only reside within the registered entity's country, if necessary or if required to do so. The customer can select what countries, regions, zones, or other demarcations around where data is stored, processed, and used. Cloud service providers also provide dashboards that provide visibility to the customer to ensure they remain fully aware of the data's location.

Registered entities using cloud technology for real-time operations will need the capability to fully assess and manage the residency of their data and will need assurance that the data is held within these areas. Appropriate selection of data residency by the registered entity, coupled with

[15] Amazon Web Services Data Residency white paper, available at https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

transparency of data residency by the cloud service provider (e.g., through dashboards) and certification of compliance with appropriate security measures by a third-party certifier, should provide adequate assurance that any data residency issues can be managed appropriately.

NERC recommends that any data residency requirements do not unnecessarily introduce any possible data resilience (e.g., availability or integrity) issues. If for national security reasons BCSI (including any data used for BES operations) must reside within the country's boundary, the cloud service provider can configure this within the cloud service provider environment accordingly and provide assurance of its configuration.

Challenges may arise that would need clear specifications regarding data residency for registered entities either spanning multiple countries or that receive real-time information from an entity in another country. This may include, for example, registered entities bordering the U.S.–Canada or U.S.–Mexico borders that share data via ICCP for use in real-time assessments or real-time monitoring that could possibly be performed in the cloud environment. In such a case, governments may need to consider pursuing agreements to help ensure the appropriate levels of data security.

C. Evaluation Criteria for Selection of Cloud Service Providers

The service level agreement between a registered entity and the cloud service provider will play a key role in establishing security if the BES reliability operating services are in the cloud. The criteria that a registered entity should prescribe in a service level agreement with a cloud service provider should mirror what the registered entity has for its non-cloud environment (e.g., logical and physical security controls, telecommunication requirements, system monitoring and support, system patching, etc.). To be most useful, registered entities should update criteria within

service level agreements and evaluate whenever new information becomes available to ensure that business goals, organizational use cases, and technical feasibility continue to be addressed.

While the criteria included in service level agreements will be important to ensuring a secure cloud environment, NERC's jurisdiction under Section 215 of the Federal Power Act limits its ability to impose any Reliability Standards requirements on cloud service providers that are not registered entities. Therefore, any breach of a security baseline included in a service level agreement would need to be addressed under the relevant contract law rather than an enforcement action involving NERC Reliability Standards. Registered entities would still be subject to the mandatory requirements under the NERC CIP standards, regardless of the existence of any breach involving a service level agreement. NERC could develop requirements similar to those in CIP-013-1 that may impact what registered entities shall require of cloud service providers in service level agreements, but ultimately the responsibility for compliance would remain with registered entities. This would be true even if, for example, the security of the cloud service provider's underlay is out of the registered entity's control.

Along those lines, third-party certifications of cloud service providers may be important to help ensure that cloud service providers are meeting security baseline criteria. Third-party certifications, such as Federal Risk and Authorization Management Program ("FedRAMP"), among others, review the security underlay of a cloud service provider's underlay environment and provide a level of assurance that the underlay is secure without every tenant hosted by the cloud service provider verifying the underlay security controls. While the ERO Enterprise may not be able to rely on third-party certifications for audit purposes without establishing a basis for that reliance (further discussed in Subsection F below), a certain security level within a third-party certification may be an important criterion to include in service level agreements between

registered entities and cloud service providers. This likely will be particularly critical given the BES reliability operating services cannot fail. That means the cloud service provider hosting the BES reliability operating services cannot fail either.

As a result, it will be important to ensure that cloud service providers meet certain security baseline criteria. NERC and industry may need to consider whether any Reliability Standards requirements can be developed to require cloud service providers meet certain criteria even though cloud service providers are not directly subject to NERC's jurisdiction.

D. Registered Entities Conducting Risk Assessments

Currently, registered entities must perform risk assessments under Reliability Standard CIP-013-1, if applicable, in planning for the procurement of BES Cyber Systems. As such, there is precedent in NERC Reliability Standards for registered entities performing risk assessments related to vendors. Nevertheless, NERC will need to consider the outcome of its supply chain standards effectiveness study to determine whether such a requirement would be appropriate for assessing cloud service providers for the different service models as described in the following table:

	Infrastructure as a Service	Platform as a Service	Software as a Service
Cloud Service Providers Responsible for:	• Hypervisors • Servers and Storage • Physical Networks	• Virtual Servers and Operating Systems • Virtual Networks • Hypervisors • Servers and Storage • Physical Networks	• Applications • Virtual Servers and Operating Systems • Virtual Networks • Hypervisors • Servers and Storage • Physical Networks

Cloud Service Customer Responsible for:	• People (using the system at the entity) • Data • Applications • Virtual Servers and Operating Systems • Virtual Networks	• People (using the system at the entity) • Data • Applications	• People (using the system at the entity) • Data

Should it be appropriate, input from industry recommended the following be included in an assessment, at a minimum:

- Ensuring operating environment is only accessible by the registered entity. The cloud service provider's employees will have various access to the cloud computing infrastructure depending on the type of service model being offered, such as Infrastructure as a Service, Platform as a Service, and Software as a Service. These varying models will need different levels of assurance from the cloud service provider and should not have access to or impact operations within the environment.
- Computing power sufficient to perform operations.
- Redundant communication pathways, in case one communication company loses the pathway.

There likely are other considerations that will be a factor in determining whether it is appropriate for registered entities to assess cloud service providers.

E. Security Responsibilities

As mentioned in the ERO Enterprise comments in response to the NOI, there are known security risks of moving BES reliability operating services into the cloud environment. Data leaks, database breaches, misconfigurations, and so on all pose risks to the confidentiality, integrity, and availability of the data and systems. While these risks also exist for networks outside the cloud, the cloud architecture, with multiple tenants using the same resources, adds complexity to these risks. In fact, while developing this informational filing, NERC became aware of instances of cloud breaches; some of these breaches involved the tenant's misconfigured applications and one involved a vulnerability with the cloud service provider. These security events demonstrate that

not only must the cloud service provider have strong controls in the underlay, but the registered entity should ensure strong controls in the overlay [16] environment as well. This shared responsibility model leverages the cloud service provider and its strong security posture to ensure security of the cloud underlay (i.e., "security of the cloud") while the registered entity will need to also have a strong security posture within the overlay (i.e., "security in the cloud"). However, as stated, ensuring security within the cloud environment will require personnel with strong cloud security expertise because moving to the cloud will increase the attack surface of systems performing the BES reliability operating services functions.

F. Compliance Oversight and Audit Processes

As noted in the ERO Enterprise comments in response to the NOI, there are aspects of the ERO Enterprise Compliance Monitoring and Enforcement Program model that currently do not rely on third-party certifications and some aspects of the shared responsibility model. For instance, if some responsibilities under the CIP requirements are delegated to the third-party cloud service provider, the ERO Enterprise would need assurances that those requirements are being met in the underlay environment. While the registered entity still holds the responsibility for compliance, the cloud service provider nonetheless may need to provide evidence to demonstrate compliance for the registered entity.

One way to gather that evidence is through third-party certifications. However, professional auditing standards include certain rules for relying on the work of others. ERO Enterprise staff are required to follow certain professional auditing standards under the NERC

[16] The overlay is the environment developed by the tenant, such as a registered entity, that includes its operations or data in the cloud.

Rules of Procedure.[17] One such set of standards is the Generally Accepted Government Auditing Standards ("GAGAS").[18] GAGAS requires auditors to employ professional judgment, bringing a certain level of skepticism to an audit to objectively review evidence.[19] Without being able to review the evidence themselves, auditors may not be able to achieve reasonable assurance of compliance. While GAGAS permits relying on the work of others, auditors would still need to determine that there is a sufficient basis for relying on that work.[20] If an ERO Enterprise auditor did not have access to the cloud service provider's certification artifacts to develop that basis for reliance, the auditor may not be able to meet obligations under GAGAS.

Given these challenges, NERC and the Regional Entities continue discussions with industry stakeholders, cloud service providers, and representatives from third-party certification organizations, such as FedRAMP, to develop solutions. During any future revisions to the CIP standards to address BES reliability operating services in the cloud, NERC would commit to working on a solution to these issues while maintaining its high standards for compliance monitoring and enforcement activities. One consideration would be a new audit process or a modified process to gather reasonable assurance that the cloud service provider's underlay is consistent with the CIP standards.

---

[17] "Compliance Audit processes for Compliance Audits conducted in the United States shall be based on professional auditing standards recognized in the U.S., which may include for example Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards and standards sanctioned by the Institute of Internal Auditors." *NERC Rules of Procedure*, Appendix 4C, Section 3.1, https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf.

[18] United States Government Accountability Office, *Government Auditing Standards* (2018), https://www.gao.gov/assets/700/693136.pdf.

[19] *Id.* Sections 3.109-3.110.

[20] *Id.* Section 8.81.

V. CONCLUSION

NERC requests the Commission accept this informational filing as consistent with the directives from the December 2020 Order. NERC will continue to consider ways to support industry in securely adopting evolving technologies as necessary, including conducting BES reliability operating services in the cloud. At this time, there is no SAR to initiate standards development or a field test, and NERC has not identified a reliability gap that would necessitate standards development to facilitate BES reliability operating services in the cloud. Regardless, NERC will continue to support entities' efforts in securely implementing emerging technologies to help ensure the reliable operation of the BPS.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

December 17, 2021

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in the above-referenced proceeding.

Dated at Washington, D.C. this 17th day of December, 2021.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American Electric Reliability Corporation