UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

JOINT COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND THE REGIONAL ENTITIES IN RESPONSE TO NOTICE OF INQUIRY

The North American Electric Reliability Corporation ("NERC") and the six Regional Entities,[1] collectively the "Electric Reliability Organization ("ERO") Enterprise," submit comments on the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Inquiry ("NOI") regarding the use of virtualization[2] and cloud computing services[3] in association with Bulk Electric System ("BES") operations.[4] Specifically, the Commission seeks comment on four areas: (1) scope of potential use of virtualization and cloud computing services; (2) potential benefits and risks associated with virtualization and cloud computing services; (3) potential impediments to adopting these technologies, including barriers within the Critical

[1] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

[2] "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." *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 at P 4 (2020) [hereinafter NOI] (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.).

[3] The NIST Information Technology Laboratory Computer Security Resource Center defines cloud computing as a "model for enabling [ubiquitous,] convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NOI at P 7 (citing NIST, *The NIST Definition of Cloud Computing*, Special Publication 800-145 at 2 (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.).

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

Infrastructure Protection ("CIP") Reliability Standards requirements; and (4) potential use of other new and emerging technologies within the existing CIP framework.[5]

The ERO Enterprise supports Responsible Entities'[6] use of virtualization and cloud computing services but recognizes there are potential risks associated with the use of these services that must be mitigated. During its engagements with Responsible Entities, the ERO Enterprise has observed varying deployment of the technologies and mitigation of the associated risks. For virtualization, the ERO Enterprise has observed Responsible Entities using virtualization and successfully mitigating known risks. For cloud computing services, the ERO Enterprise has only just started seeing Responsible Entities use cloud services for data storage of BES Cyber System Information ("BCSI") and has not observed Responsible Entities use cloud computing services for BES reliability operating services, Electronic Access Control or Monitoring System services, or Physical Access Control System services.[7]

While the ERO Enterprise recognizes that Responsible Entities may want to use cloud computing services for more components of their operations, the ERO Enterprise stresses the need for Responsible Entities to be cognizant of the risks and to implement mitigating actions to help ensure the security of the Bulk-Power System ("BPS").

---

5 NOI, *supra*, at P 14.

6 As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

7 For purposes of these comments, BES reliability operating services refers to the following as listed in the NOI at P 16:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

The ERO Enterprise recognizes that there may be benefits to using these technologies, as highlighted in the NOI. In these comments, however, the ERO Enterprise focuses on some of the risks of these technologies that would need to be mitigated if the technologies were implemented, particularly with respect to BES reliability operating services. These comments are not intended to provide an exhaustive list of all potential risks associated with the use of these technologies or to advocate for a particular risk mitigation strategy. Work is currently underway, through NERC's industry-driven standard development process and through ERO Enterprise outreach to industry groups, to continue to identify the potential risks and effective mitigation strategies, taking into account all relevant considerations. NERC anticipates that the comments received by the Commission during this NOI proceeding will help inform these efforts.

These comments are organized into the following sections: Section I.A provides ERO Enterprise identified risks associated with virtualization; Section I.B provides ERO Enterprise identified risks associated with cloud computing services; and Section I.C describes the current standards development projects related to virtualization and cloud computing services as well as efforts to address other emerging technologies. Section II provides a conclusion to these comments.

I. COMMENTS

In the NOI, the Commission seeks comment on the risks associated with virtualization and cloud computing services. In question B2 of the NOI, the Commission asked whether there are risks associated with adopting virtualization for BES reliability operating services.[8] Question B4 asks whether there are risks associated with adopting cloud computing services for BES reliability

[8] NOI, *supra*, at P 18.

operating services, data storage, and support services.[9] Question B6 asks commenters to discuss risks associated with relying on third-party assessments to ensure the secure use of virtualization and cloud computing services for BES reliability operating services and support services.[10]

In these comments, the ERO Enterprise provides comments mainly on the risk-focused questions from the NOI described above.[11] The ERO Enterprise supports Responsible Entities' use of virtualization technologies and, in limited circumstances, cloud computing services if appropriate controls are in place to address the risks listed below.

The Commission posed other questions in the NOI regarding benefits of these technologies, methods to mitigate risks, and how the CIP Reliability Standards could inhibit adoption of these technologies. However, because NERC currently has standards development projects underway to address these issues, as described in Section I.C below, the ERO Enterprise does not comment on the remaining questions from the NOI at this time.

A. The ERO Enterprise supports Responsible Entities' use of virtualization technologies, even in performing BES reliability operating services, if appropriate controls are in place to mitigate risks and vulnerabilities.

The ERO Enterprise identified risks posed by the use of virtualization technologies that would need mitigating actions if implemented. Virtualization allows multiple virtual machines to independently utilize the shared memory, storage, and compute resources of a single physical host. These hosts could be configured with different levels of trust, creating a shared infrastructure.

---

9 *Id.*

10 *Id.*

11 These include questions B2, B4, and B6. Relevant to NERC, the Commission also poses questions regarding these technologies' interaction with the CIP Reliability Standards. Question C2 asks whether there are any technical challenges in implementing virtualization technology for the BES reliability operating services regarding cloud computing services. Questions C3 and C5 ask whether there are any challenges in implementing virtualization or cloud computing technology for the BES reliability operating services that result from compliance obligations associated with the CIP Reliability Standards. Finally, question D1 asks commenters to discuss whether the CIP Reliability Standards limit the ability to take full advantage of new and emerging technologies for BES reliability operating services.

While ERO Enterprise staff have seen Responsible Entities using virtualization technologies during engagements and recognize the resiliency, efficiencies, and economies of scale achieved by these Responsible Entities, the ERO Enterprise identified the following risks of virtualization technology.

Data Security: While data security is an inherent concern with information technology, virtualization technologies present unique risks to data security. Specifically, hosts sharing the same infrastructure can create vulnerabilities if certain risks are not addressed. If these hosts have different trust levels, there is a risk that unauthorized access could occur to data in higher trust levels unless appropriate protections are in place. For instance, a misconfiguration could allow unauthorized personnel to obtain access to high security virtual machines or hypervisors, the underlying hardware that could impact all the virtual hosts.

The use of images in virtualization technologies further creates data security challenges that Responsible Entities would need to mitigate. An image is defined as, "[a] file or directory that contains, at a minimum, the encapsulated components of a guest [operating system]."[12] In virtualization, it is relatively easy to create, run, and delete images. With the large number of potential images and their ephemeral characteristics, there is a risk that these images may not receive the appropriate security controls. Patching is one example. If these virtual hosts are reloaded for use without receiving updated patches, there is a risk that the virtual hosts do not receive the latest security updates, thereby lowering the level of data security for the system. Furthermore, images are often copied from a base image, or "gold standard." If there is a misconfiguration in the base image, there is a risk of propagating the misconfiguration in all copies.

[12] NIST, *Guide to Security for Full Virtualization Technologies*, *supra*, at A-1.

Finally, there are other risks to data security posed by virtualization technology characteristics. Virtual machines are often run through a test or pre-production environment prior to being used in the production environment. Changing from a pre-production to production environment for virtualization often requires a simple configuration change. If not configured properly, there is a risk of a pre-production, unsecure virtual machine running in a production environment. These unsecure virtual machines could lead to resource consumption, degradation of system performance, and increased risk of exposure.

Complexity: Virtualization presents unique challenges in terms of complexity. Complexity refers to multiple components interacting with one another in a variety of ways. In particular, the virtualization networking infrastructure necessitates more layers[13] than that of a non-virtualization solution. This adds complexity and the potential loss of visibility to the infrastructure. As such, the complexity of these additional layers can make it more difficult to spot anomalies or unusual events happening on the network and the virtual machine. If the complexity is unmanaged, there is a risk that malicious actors could orchestrate an attack without being detected.

For instance, hosts only have a finite amount of resources available, and virtual hosts compete for the same resources, such as central processing units and memory. If an overprovisioning of host resources occurs, Responsible Entities could experience service impacts if the overprovisioning is not addressed appropriately. For BES reliability operating services, this could cause a problem in slowing down these operations when needed. For example, a virtual system that may be running a BES reliability operating services function could be placed at a lower priority and would operate in a degraded manner, thus impacting BPS reliability.

[13] "Layers" are used to describe the different functions within a network that work together to make the network communications operate (e.g., physical layer to application layer).

Moreover, the hypervisor can pose risks given its core function in creating a virtualization environment. As noted in the NOI, the hypervisor is the "centralized software… that manages multiple virtual computer resources that can be used by different processes, customers, clients, and users."[14] Based on this centralization, there is a risk that a hypervisor can become a single point of failure for numerous virtual machines if not properly configured for redundancy. Additionally, there is a risk of a bare metal hypervisor[15] becoming oversubscribed without proper planning and baselining, which could result in loss of a virtual machine's sufficient functioning. For example, anti-virus and other security software may not be effective in monitoring or preventing security incidents because the system may be suffering from resource exhaustion. If the system is suffering from resource exhaustion, it may not respond quickly enough, or at all, due to it being overloaded.

Finally, dormant virtual machines may cause issues if not managed appropriately. Dormant virtual machines could be using up a network's resources, lowering the level of reliability of the network. Furthermore, these dormant machines could be behind on patching, creating an even larger exposure and vulnerability for the network.

Despite these potential risks, the ERO Enterprise supports Responsible Entities' use of virtualized technologies, even in performing BES reliability operating services, if appropriate controls are implemented to mitigate the risks and vulnerabilities discussed above, in addition to other risk and vulnerabilities not specifically addressed herein.

---

[14] NOI, *supra*, at P 4.

[15] This type of hypervisor is installed directly on the physical hardware, as opposed to a hypervisor running on a host operating system.

B. The ERO Enterprise currently supports Responsible Entities' use of cloud computing, in limited circumstances and with the appropriate controls in place, to mitigate risks and vulnerabilities. Looking forward, the ERO Enterprise would be open to further uses of cloud computing if the appropriate controls are implemented.

The ERO Enterprise supports use of cloud computing for data storage of BCSI as the risks posed by third-party services for data storage listed below can be appropriately mitigated. Furthermore, the ERO Enterprise could support use of cloud computing for BES reliability operating services if appropriate protections are in place to mitigate risks and vulnerabilities. As virtualized environments provide the foundation for cloud computing services, the ERO Enterprise notes that the risks described in Section A above apply to cloud computing services as well. The following section provides additional risks to be addressed in cloud computing.

ERO Enterprise staff has observed that some Responsible Entities use cloud computing services for data storage, including BCSI storage. While ERO Enterprise staff has not seen Responsible Entities using cloud computing technology, particularly third-party cloud computing services, for BES reliability operating services, the ERO Enterprise recognizes that certain support services are increasingly being offered through cloud computing services. As such, while the ERO Enterprise is open to understanding how these technologies can support BPS reliability, the ERO Enterprise has identified the following risks posed by use of cloud computing services that need mitigating actions if implemented.

Data Security: Similar to virtualization, there are data security risks for cloud computing services that result from its unique infrastructure. Some of the efficiencies of the cloud come from tenants sharing resources with one another. As such, there is a risk if the data is not protected appropriately. For instance, without proper encryption management, data at rest and in transit could be at risk if it is unencrypted or uses inadequate encryption, including aged or inadequate ciphers. Likewise, Responsible Entities would need to ensure that the cloud service provider uses

security protections for data in use as well. The risk of not protecting data appropriately is that a third party could gain unauthorized access to BCSI, including access to data in use. In particular, unauthorized access to BCSI is a concern because, by definition, BCSI can be used to gain unauthorized access to BES Cyber Systems or pose a security threat to them.

In terms of data security, there are also risks based on the way the cloud service provider structures its business and services.[16] First, cloud service provider agreements may place limits on a Responsible Entity's ability to manage or control data or its geographical location. Second, a cloud service provider could create risk if any misconfigurations permit unauthorized access to data. Finally, cloud applications undergo constant feature additions, and there is a risk if Responsible Entities do not keep up-to-date with application improvements to ensure protection of their data.

In addition, there is a risk that data, if not disposed of properly by the Responsible Entity, may end up in storage of another tenant. This could happen as cloud service providers share resources among tenants. In cloud services, many devices are used for efficiency and resilience. Data from one tenant is often stored over several different storage devices within the cloud service provider's infrastructure. This infrastructure supports multi-tenancy environments, so data from one entity is spread across several devices with other tenants' data. If a Responsible Entity's data is not disposed of properly, it could remain in the storage resource, leaving it potentially accessible to other tenants that use that space.

Quality of Service and Resiliency: In cloud computing, Responsible Entities are sharing resources with other tenants. Depending on all the tenants' usage and demands on these resources,

[16] As noted in the NOI, there are three main cloud service models that provide different levels of control for Responsible Entities: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). NOI at P 8.

there may be impacts to quality of service. Quality of service is the performance, availability, and reliability offered by the cloud service provider. Responsible Entities can contract for a certain level of quality of service in their agreements with cloud service providers. However, as described below, there may be some challenges to achieving the type of quality of service needed, particularly if Responsible Entities were to use cloud computing services for BES reliability operating services.

Quality of service depends in part on the telecommunication paths between the Responsible Entity and the cloud service provider. Many of these telecommunications paths are not under the control of the Responsible Entity and may in fact be owned and controlled by a third party other than the cloud service provider. Consequently, neither the Responsible Entity nor the cloud service provider would have direct control over the availability and reliability of these paths to help ensure the appropriate quality of service. While companies can pay for a guaranteed level of quality of service, there could still be issues if demand for these services continues to grow. The guaranteed level of quality of service could become more expensive based on this demand. As such, Responsible Entities may not always be able to control the quality of service needed for BES reliability operating services.

In addition, there are risks to resiliency if multiple Responsible Entities use one major cloud service provider. For instance, there could be an impact to the BPS if that major cloud service provider had technical issues affecting availability or was otherwise compromised. This could be a single point of failure, resulting in the loss of multiple Control Centers at the same time.

ERO Enterprise Oversight: The ERO Enterprise could lose visibility into certain activities of Responsible Entities using the third-party cloud environment. In cloud computing, Responsible Entities would move to a shared responsibility model to help ensure BPS reliability and security.

A shared responsibility model means that Responsible Entities and cloud service providers would share tasks and controls to meet security obligations. This model conflicts with the way compliance is currently handled by the ERO Enterprise. If Responsible Entities started using cloud computing services even more, there is a risk that the ERO Enterprise could lose visibility and oversight into some of the Responsible Entities' activities.

Moreover, while there are ways to gain oversight into cloud service providers through third-party assessments or certifications, there is a risk that these methods will conflict with the obligations of ERO Enterprise staff. ERO Enterprise staff are required to follow certain professional auditing standards under the NERC 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 in order 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.

---

[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* (July 2018), https://www.gao.gov/assets/700/693136.pdf.

[19] *Id.* Section 3.110.

[20] *Id.* Section 8.81.

Infrastructure and Operations: There are risks that stem from cloud service providers' operations and infrastructure. In contrast to many Responsible Entities' current configurations, particularly for BES reliability operating services, Responsible Entities would have to engage in more Internet-facing activities if using cloud computing services for their operations. Increasing the Internet-facing activities increases the exposure of these sensitive systems which can increase the risk to the BPS. The risks of Internet-facing activities have long been a focus of security protections and are addressed in the current CIP Reliability Standards. As a result, many Responsible Entities would need to reconsider their security configurations and be sure to address these risks if using cloud computing services.

There also are risks in the way a cloud service provider structures its operations, infrastructure, and maintenance. For example, if the cloud service provider outsources parts of its operations, infrastructure, or maintenance to a third party, there is a risk this third party may not be able to support or carry out the requirements that the cloud service provider is contracted to provide to a Responsible Entity.

C. Ongoing standard development projects 2016-02 and 2019-02 are proposing revisions to the CIP standards to address virtualization and cloud computing storage for BCSI.

As the Commission recognized in the NOI, NERC has ongoing standards development projects to revise the CIP suite of standards to address virtualization and storing BCSI with cloud service providers. The standard drafting team for Project 2016-02 – Modifications to CIP Standards is developing revisions to the CIP standards to help address areas where requirements can better support the appropriate protection configuration for virtualization technology to mitigate

the above risks.[21] The standard drafting team for Project 2019-02 – BCSI Access Management is developing modifications to the CIP Reliability Standards regarding managing access and securing BCSI.[22] NERC submitted informational filings regarding the status of these projects in Docket No. RD20-2-000.[23]

The standard drafting teams for these projects recognize the benefits of these technologies and continue to identify areas in the CIP Reliability Standards that can support them. During development, ERO Enterprise staff have been engaged in discussions to help ensure the risks discussed above are considered by the standard drafting teams. Because these projects are currently ongoing, however, the ERO Enterprise declines to further comment on areas where the standards could be revised or how these risks are being addressed. NERC will discuss any relevant revisions addressing the risks above in petitions for approval of CIP Reliability Standards revised by these standard drafting teams, as applicable.

During revisions of the CIP Reliability Standards throughout the past decade, the ERO Enterprise has recognized the rapid pace of emerging technologies. As such, the ERO Enterprise supports the "future-proofing" of standards such that the language will not prohibit use of emerging technologies but will help to ensure cyber security principles apply and remain requirements. In particular, the Project 2016-02 standard drafting team has focused on revising the requirements in a way where the controls are not overly prescriptive where possible.

---

[21] The web page for Project 2016-02 is available at https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

[22] The web page for Project 2019-02 is available at https://www.nerc.com/pa/Stand/Pages/Project2019-02BCSIAccessManagement.aspx.

[23] NERC, *Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 19, 2020); NERC, *Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (Mar. 19, 2020).

II. CONCLUSION

As discussed above, the ERO Enterprise supports Responsible Entities' use of virtualization and cloud computing services if appropriate controls are in place. The ERO Enterprise continues to work with industry, through standards development projects and other activities, to help ensure the risks described above are addressed and mitigated if needed.

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, DC 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: July 1, 2020