STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

| | |
|---|---|
| Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data | Case 20-M-0082 |

**ARCADIA'S COMMENTS ON THE JOINT UTILITIES' PETITION TO MODIFY SELF-ATTESTATION REQUIREMENTS**

Dated: July 25, 2022
Albany, New York

## I. Introduction

In their May 3, 2022 *Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self Attestation Updates* ("Petition"), the Joint Utilities request that the New York State Public Service Commission ("Commission") make certain modifications to its October 17, 2019 *Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings* ("Cybersecurity Order").[1] Specifically, the Joint Utilities request an update to six existing requirements and three new requirements in the current Self Attestation ("SA") of the Commission-approved Data Security Agreement, while also seeking a modification to permit a governance process for periodic SA review and to provide recommendations for further SA updates. On May 25, 2022, the Department of Public Service noticed the Petition in the New York State Register with public comments on the Petition to be received by July 25, 2022.

Arcadia Power, Inc. d/b/a Arcadia,[2] respectfully submits these comments to the Commission in response to the Petition. Arcadia fully agrees that cybersecurity protections "must keep pace with the best practices, technology, and industry requirements."[3] In an increasingly interconnected world, cybersecurity standards evolve at a pace that requires constant adaptation to maintain the appropriate amount of vigilance and security. This reality puts the entire system's security dependence at risk when it is predicated on a self-attestation process alone.

Instead, the Commission should reconsider using a risk-based approach to cybersecurity, whereby any activity with a perceived higher risk requires Energy Service Entities ("ESEs") to implement correspondingly higher standards of cybersecurity processes and protocols. The Commission recognized the merits of a fully risk-based approach to cybersecurity in its 2019 Cybersecurity Order, but concluded that it needed to conduct more analysis on frameworks before adopting such an approach.[4] Given the changing realities since the Cybersecurity Order was issued in 2019, Arcadia respectfully asks the Commission to reconsider a risk-based approach while considering the requested modifications to the SA process.

In addition to the general request to adopt a risk-based approach to cybersecurity that includes the SA, we recommend the Commission remove or modify the current SA requirement that all confidential customer utility information be stored in the U.S. or Canada only (Cybersecurity Protection 10). Such a blanket restriction is not informed by risk level and is also

[1] Cases 18-M-0376 et al., *Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings* (Oct. 17, 2019) ("Cybersecurity Order").
[2] In 2019, Arcadia Power rebranded to Arcadia.
[3] Petition at 2.
[4] Cybersecurity Order at 35-36.

premised on a flawed understanding of zero trust architecture. There are better ways to address national security concerns related to data processing than implementing such an overly broad geographic restriction. To the extent there is any actual, incremental risk associated with processing data outside of the U.S. and Canada, there are numerous mitigation measures under a risk-based framework that would offset such a perceived risk. At a minimum, ESEs should be allowed a waiver from these unduly burdensome geographic restrictions upon implementing risk-based mitigation measures that more fully address the data processing security risks at the core of that policy's rationale.

We also echo comments made in Mission:data's response to this Petition that the root cause of this matter is the Joint Utilities' liability for customer-authorized third party data breaches. In order to follow best practices established by other states, Arcadia requests that the Commission conclusively removes liability from the Joint Utilities for customer-permissioned third-party data breaches. Finally, we urge the Commission to establish a right to due process for ESEs with respect to cybersecurity standards while also requiring ESE representation on the proposed Governance Committee.[5]

## II. Arcadia Recommends Developing a Risk-Based Approach to Increase Data Security

We agree with the Joint Utilities' assertion that the process by which cybersecurity risks are assessed should be a constant and evolving process to ensure grid resiliency, security, and protections to customer data. In furtherance of this objective, we encourage the Commission to use the Petition as an opportunity to enhance cybersecurity by implementing foundational frameworks (i.e. risk-based) endorsed by the National Institute of Technology and Science ("NIST"). NIST consistently advocates for an embrace of a risk-based approach to data security whereby varying levels of cybersecurity scrutiny and rules are dependent on the risk-level associated with a particular activity. Indeed, many of the recommendations made by the JUs to modify the Self Attestation are NIST standards.

Rather than establishing a static, prescriptive set of requirements that ESEs must attest to have met, the Commission could both enhance data security and provide greater flexibility by adopting a risk-based approach. A risk-informed audit process like SOC 2 would help better protect against cybersecurity risks because it is far more capable of adapting to the changing nature of threats. Rather than having an ESE self-attest to satisfying certain set requirements that would inevitably suffer from regulatory lag, a risk-based approach would be more flexible, and more effective at ensuring customer data is protected. A self-attestation process could have a role in such an approach, but it would serve as just one element and typically for protecting lower-

[5] Response of Mission:data Coalition to *Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates.*

risk activities. Third-party audits, rather than self-attestations, ensure a greater level of accountability, and relying on an SA alone for higher-risk activities would be inadvisable. Moreover, the Commission agrees in the Data Access Framework Order that self-certification is "no longer a sufficient means by which to verify the appropriate protections are in place to safely protect systems and customer privacy."[6] Accordingly, the Commission should take any necessary interim action to bolster cybersecurity protocol in response to this Petition and in anticipation of the transition to the Data Certification Process.

## III. Arcadia Requests Reconsideration of Cybersecurity Protection 10 to Allow for Modern Data Storage and Processing Practices

The Petition leaves unmodified the DSA's Cybersecurity Protection 10, which states, "All Confidential Customer Utility Information is stored in the United States or Canada only, including, but not limited to, cloud storage environments and data management services (Inconsistent with "zero trust architecture")."[7] This blanket geographic restriction does not take into account relevant cybersecurity threats to confidential customer data, but nonetheless imposes a significant and disproportionate burden on ESEs seeking to leverage data to enhance DER offerings. Such a blunt, categorical requirement is not informed by risk level and is an outlier amongst states. As discussed below, it is also based on a flawed justification and understanding of the meaning of the Zero Trust Architecture framework.

### A. Limiting Data Processing to the U.S. and Canada is Arbitrary and Lacks Support in the Record

The record in this proceeding provides scant justification for prohibiting storage of data outside of the U.S. and Canada. In their February 2019 DSA Petition, the Joint Utilities asserted this requirement was necessary to comply with United States Export Administration Regulations and the International Traffic in Arms Regulations, stating:

> the United States Export Administration ("EAR") (15 C.F.R. §§730-774) and the United States International Traffic Arms Regulations [sic] ("ITAR") (22 C.F.R. Section (§) 120-130) permit covered information to be stored in the United States and Canada, but not elsewhere. The Joint Utilities have consistently indicated that they will consider requests for storage in other countries if the ESE can demonstrate compliance with EAR and ITAR.[8]

---

[6] Case 20-M-0082, *Order Adopting a Data Access Framework and Establishing Further Process* (Apr. 15, 2021), at 16.

[7] Petition, Appendix A (No. 10).

[8] Case 18-M-0376 at al, *Joint Utilities' Petition for Approval of the Business-to-Business Process Used to Formulate a Data Security Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce*

These regulations are not applicable to utility data. First, it is unreasonable to hold ESEs accessing utility customer data to the same cybersecurity standards imposed by the United States Export Administration Regulations given the nature of the actual cybersecurity risk that customer's energy data actually poses on national security. The ITAR is intended to govern the import and export of defense and military technologies.[9] Utility customer information does not meet ITAR's definition of "technical data," which includes information "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles," and software "directly related to defense articles."[10] Neither EAR nor ITAR are relevant justifications for cybersecurity protections in the SA.

Second, even if the EAR were a relevant regulatory framework, the utilities appear to have arbitrarily restricted data processing to the U.S. and Canada, exceeding the limits imposed by the EAR. The U.S. Commerce Department's Bureau of Industry and Security ("BIS"), which implements the EAR, has a comprehensive grouping system to categorize countries. The Country Groups (*i.e.*, A, B, D, E) reflect each country's export control policy, multilateral regime membership, system, and practice, and generally serve as a basis for the availability of license exceptions under the EAR.[11] These Country Groups range from high-risk countries in Groups E (i.e., terrorist supporting countries or unilaterally embargoed countries such as Cuba, Iran, North Korea, and Syria) to low-risk countries in Group A (listing over 50 countries) and Group B, which includes U.S. allies such as Sweden, Spain, Finland, and Ireland.[12] This list is vetted and updated frequently by experts who understand the nature of geopolitical threats, and it is based on the changing nature of threats and political exigencies.

We maintain that a risk-based framework is preferable to any arbitrary geographical restriction, and we acknowledge the concerns animating the BIS's Country Groups are separate from utility customer data-related concerns. However, the BIS Country Groups would be a more grounded reference for data processing geographical restrictions than one arbitrarily limited to the U.S. and Canada. If the Commission determines the DSA must contain a geographic restriction, it should include a risk-based approach that grants an ESE a higher threshold of acceptable activities if said ESE can demonstrate correspondingly enhanced cybersecurity standards and protocols. For instance, the Commission should restrict data processing in Group E countries on BIS Country Group list, *i.e.*, designated terrorist supporting countries and Cuba,

---

*Execution of the Data Security Agreement by Entities Seeking Access to Utility Customer Data or Utility Systems* (Feb. 4, 2019), Attachment 3, at 13.

[9] The ITAR implement the President's authority "to control the export and import of defense articles and defense services" and promulgate regulations with respect thereto. *See* 22 CFR § 120.1(a).

[10] *See* 22 CFR § 120.10(4).

[11] *See* Dep't of Commerce Bureau of Industry and Security, *Amendment to Country Groups for Ukraine, Mexico, and Cyprus Under the Export Administration Regulations*, 85 Fed. Reg. 84,211 (Dec. 28, 2020), https://www.govinfo.gov/content/pkg/FR-2020-12-28/pdf/2020-26552.pdf.

[12] Bureau of Industry and Security, *Supplement No. 1 to EAR Part 740* (June 2, 2022), https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-country-groups-1/file

which is subject to a unilateral embargo. However, the Commission should allow data processing in countries found in Groups A and B so long as those ESEs adopt correspondingly stronger cybersecurity protocols, such as maintaining SOC 2 compliance.

We reiterate that the Joint Utilities do not state why ESEs accessing customer energy usage data should be subjected to the same regulations that govern international arms trafficking or exports of military technology. On its face, this is an overly conservative approach to data security, particularly as it relates to processing customer energy usage data. As a result, this restriction will severely limit the ability of ESEs to innovate, drive down costs, and provide increased savings to customers.

### B. Zero Trust Architecture Framework Does not Justify the U.S. and Canada Data Storage Restrictions

The Joint Utilities have also claimed that Cybersecurity Protection 10 in the Self-Attestation form is necessary to maintain consistency with Zero Trust Architecture,[13] but this fundamentally misunderstands the nature and purpose of Zero Trust Architecture. As explained in NIST's Special Publication 800-207 on Zero Trust Architecture:

> Zero trust assumes there is **no implicit trust granted to assets or user accounts based solely on their physical or network location** (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)... Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. **Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.**"[14]

Under a Zero-Trust Architecture, which has been nearly universally endorsed by NIST as the preeminent cybersecurity framework, the security perimeter is no longer the network connection or environment, but is instead the end-point device, such as mobile phones or laptop computers. This means that the geographic location of the end-point device has less bearing on the relative security of a network because Zero-Trust Architecture (ZTA) is built to de-emphasize network location and instead require multiple layers of authentication for the end-point client that "move defenses from static, network-based perimeters to focus on users, assets, and resources."[15] Accordingly, the relative geographic location of where the data is being

[13] Petition, Appendix A (No. 10) ("(Inconsistent with "zero trust architecture")").
[14] NIST, *Special Publication 800-207 on Zero Trust Architecture* (Aug. 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, at ii (emphasis added).
[15] *Id.*

processed is a relatively less vital component of ensuring cybersecurity under ZTA and should be reconsidered.

### C. Current Geographic Restrictions on Data Processing Impose Undue Costs on Operations Ultimately Borne by Customers

The offshoring requirement creates significant operational costs for ESEs. Put simply, the restriction against processing data outside the U.S. and Canada limits the pool of labor the industry can employ to process data, which has a direct impact on the industry's ability to serve New York customers with the best and most competitive energy products. Arcadia, for example, is a globally-connected technology company with a substantial platform designed to leverage the potential of utility customer energy data. Arcadia has over 300 team members in India, and another team in the Philippines. With the current DSA restrictions, we are unable to use these talented resources and either must make bespoke, state-specific security arrangements that raise the costs of our New York products or limit what we can do in the state.

As a data-driven, technology company, Arcadia takes data protection very seriously. Indeed, we welcome requiring more stringent auditing measures beyond SAs because robust protections for customer data and the safety of utility IT systems are needed. However, offshoring limitations do little to enhance cybersecurity while adding a significant cost to the ESE and New York customers. We urge the Commission to take this "net impact" effect on the ability to serve customers into consideration.

## IV. New York's SA Approach is Out of Line with Best Practices in Other States

To our knowledge, no other state has geographic restrictions for energy service entities when accessing customer energy usage data. This seems to be a New York-specific requirement.

For example, the New Hampshire Public Utilities Commission recently approved a settlement agreement dictating the terms of cybersecurity requirements for any energy service company seeking to access customer's energy data.[16] Notably, the settlement contains no geographic restrictions on where data can be processed or stored. Moreover, the agreement also employs a risk-based approach to data access and cybersecurity. Appendix C of the Settlement Agreement outlines 4 risk-based groups that are segmented depending on the expected data that will be accessed from the platform, with groups with perceived higher risks (based on volume of accounts accessed) having more stringent cybersecurity requirements.[17] For instance, one of the requirements for processing high-risk datasets (if a third-party hosting service is used) is that an

[16] New Hampshire Public Utilities Commission, *Order Approving Settlement and Establishing a Process for Developing a Statewide Data Platform*, Order No. 26,589, Docket No. DE 19-197 (Mar. 2, 2022).
[17] *See Settlement Agreement*, Docket No. DE 19-197 (Apr. 28, 2021), Appendix C.

energy service entity must describe their controls and attach a SOC 2 audit report or other document summarizing their physical security control.[18]

This framework appropriately accounts for perceived higher-risk activities with corresponding higher requirements. Such an approach obviates the need to restrict where data is processed while also establishing a precedent for requiring higher-risk activities to implement correspondingly higher protections and cybersecurity protocols to protect data so long as those protocols are in accordance with SOC 2 trust service principles.

Though the Commission elected not to adopt a fully risked-based approach to cybersecurity and data privacy in their Cybersecurity Order, it did recognize the eventual necessity for such a framework upon conducting more analysis, "In order to implement a more detailed risk analysis approach for further consideration, with the potential of performing a fully risk-based assessment for each ESE, applicable frameworks for cybersecurity and data privacy need to be identified and analyzed."[19] We encourage the Commission to take the Petition as an opportunity to make incremental steps toward a risk-based framework.

## V. The Data Security Agreement Should Require SOC 2 Type I Compliance

The current Data Security Agreement contains 15 mandatory checks that an ESE must comply with in order to be deemed to have sufficient cybersecurity controls in place. SOC 2 compliance, a higher standard for ensuring compliance with a company's own customer data security protocol, is currently an optional requirement.

The Commission's *Order Adopting the Data Access Framework* anticipates a future in which all companies will have to maintain some level of audit compliance – either via SOC 2 Type II compliance or via an audit conducted by a yet-to-be-determined Data Ready Certification Provider. The Commission recognizes in the Data Access Framework that self-certification of cybersecurity protections is "no longer a sufficient means by which to verify the appropriate protections are in place to safely protect systems and customer privacy."[20] Moreover, the Data Ready Certification process currently being developed alludes to the future need for "ESE's submission of independent recognized security controls audit report."[21]

Given the eventual transition toward a mandatory audit compliance mechanism under the Data Certification Process, Arcadia recommends that at a baseline, SOC 2 Type I compliance be a mandatory requirement.

[18] *Id.*, Appendix C-1, at 12.
[19] Cybersecurity Order at 35-36.
[20] Data Access Framework Order at 16.
[21] *Id.*

The Joint Utilities acknowledged that their proposal is timely given the Commission's expectation to begin implementation of the Data Access Framework and Data Ready Certification ("DRC") Process in 2022. If SOC 2 Type II compliance (requiring continuous third-party audits to ensure internal ESE controls are being properly maintained) is expected to be a data security requirement for the implementation of the DRC process, requiring that ESEs at a baseline establish SOC 2 Type I Compliance (requiring ESEs establish and abide by internally designed ESE controls at a single moment in time) in the interim seems like a logical progression toward ensuring all ESEs are prepared for the eventual transition to the DRC process.

In general, moving cybersecurity controls and processes toward a certification-based process (as opposed to a self-attestation process) is preferable given standardization of application across ESEs and a higher degree of data security relative to the SA process, which is inherently subjective. SOC 2 is a more accountable standard given that it is an audit process verified by a third-party as opposed to a self-reported process.

Moreover, many of the proposed revisions in the JUs Petition replace existing language around "industry-standard" practices to that of well-established cybersecurity frameworks such as NIST standards and guidelines. NIST itself advocates for a risk-based approach to cybersecurity, so if the JUs are insistent on citing NIST standards, it is only consistent to also advocate for their foundational premise of risk-based cybersecurity standards. Further, the proposed changes to well-defined cybersecurity standards is aligned with the Commission's express position to potentially adopt a "more prescriptive standard at a future date." as it pertains to cybersecurity standards. (Cyber Security Proceeding, Minimum Protections Order, p. 49.) Similarly, a requirement for all ESEs to be SOC-II Type 1 compliant further establishes a foundation of requiring industry standards and best practices as opposed to a more subjective and less robust Self-Attestation process around cybersecurity.

## VI. Arcadia Requests Modifications to the Proposed Changes to Cybersecurity Protection #6 on Anti-Virus Software

The JU's proposed modification to Petition Item #6 on Anti-virus Software would "Require installation of Endpoint protection software on all servers and workstations and maintenance of same with up-to-date signatures." The JUs add that this "this change reflects that Endpoint protection, which includes antivirus software, is now the recommended technology for handling virus protection."

Many companies today, including Arcadia, use a modern tech stack that is based on "containers" not servers. Put simply, containers provide more flexibility and portability of applications that are necessary in multicloud environments; containerizing applications provides organizations with more freedom to deploy applications in the many software environments of today's virtual world. Moreover, containers are increasingly utilized by the technology industry.

"Endpoint protection" is not a suitable solution for containers. That said, containers deployed in a typical immutable configuration are inherently more secure than most server and workstation configurations. Accordingly, we propose that the Commission consider an alternative to satisfy the requirement by specifying an alternative mitigating control. Thisapproach has been adopted recently in the 4.0 version of PCI, which is related to credit card info security requirements. We respectfully request that the Commission consider the realities of emerging best practices for container-based tech stack vs. server-based tech stack and permit suitable protections that are applicable for all technologies.

## VII. The Proposed Governance Committee Should Include ESE Representation While Establishing a Right to Due Process for ESEs

In the Petition, the Joint Utilities propose that the Commission establish a Governance Committee, which would, among other things, "(1) consist of up to five representatives of the Joint Utilities and up to five representatives of Department of Public Service Staff (Staff), all of whom are cybersecurity subject matter experts; (2) meet at least quarterly; (3) establish an advisory working group to provide the Governance Committee with suggestions, recommendations, and feedback on further updates to the SA; (4) consider the current threat landscape, existing regulatory and legislative framework, and identify risks and potential gaps in current cybersecurity protections; (5) recommend changes to the SA requirements to the Commission, as needed; and (6) participate and engage with stakeholders."[22]

The creation of a Governance Committee is an excellent opportunity – however, the proposed committee is seriously flawed. The JU proposal is to have zero representation from the ESE community. Given that ESEs are the entities that sign the Data Security Agreement and that ESEs are responsible for implementing the cybersecurity protocols that are ostensibly overseen by a Governance Committee, any Committee must have equal representation from ESEs. Moreover, the powers with which the Governance Committee would be vested would undermine both the Commission's authority as well as ESEs' due process rights before the Commission by requiring that the Commission act on the Commission's recommendations within four (4) months of issuance. Moreover, we concur with the comments filed by Mission:data to this proceeding:

> The casualties of a shortened timeframe for a final decision by the Commission would be ESEs, who would have extremely limited opportunity to exercise their due process rights. Not only would ESEs have slim opportunities for comment on the Joint Utilities' proposed timeframe, but it would be impossible to challenge the ever-changing requirements of the Joint Utilities through discovery, testimony, cross-examination, or an evidentiary hearing before the Commission. The Petition would, if granted, enshrine a

[22] Petition at 10.

short-circuited procedure that deprives the Commission of exposure to dissenting views and new information that are the basis for sound decision-making.[23]

At the core of this issue is ESEs right to due process. Arcadia's strong recommendation is to make this proposal workable by including five representatives from ESEs on the Governance Committee while also ensuring that a right to due process for ESEs is firmly established . Otherwise, this promising proposal must be ignored.

## VIII. Conclusion

We respectfully submit these comments and thank the Commission for their time and attention on this vital issue. We look forward to continued engagement on this discussion.

**ACADIA POWER INC. d/b/a ARCADIA**

**/s/**

Austin Perea
New York Policy Manager
115 W 18th St
New York, NY, 10011
Tel: (603) 370-7811
Email: austin.perea@arcadia.com

[23] Mission:data Response to Petition to Modify DSA at 4-5