July 22, 2022

**Via E-Docket**

Hon. Michelle L. Phillips, Secretary to the Commission
New York State Public Service Commission
Empire State Plaza, Agency Building 3
Albany, NY 12223-1350
secretary@dps.ny.gov

**Re: Case Nos. 18-M-0376 and 20-M-0082**

Please find enclosed the Response of Mission:data Coalition to the Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates. If you have any questions about this submittal or have difficulty viewing the enclosed PDF, please contact me.

Respectfully submitted,

**Michael Murray, President**
Mission:data Coalition
1752 NW Market St #1513
Seattle, WA 98107
(510) 910-2281 (phone)
michael@missiondata.io

**STATE OF NEW YORK**

**PUBLIC SERVICE COMMISSION**

| | |
|---|---|
| Proceeding on Motion of the Commission Regarding Strategic Use of Energy Data | Case 20-M-0082 |
| Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place | Case 18-M-0376 |

**Response of Mission:data Coalition**

**To the Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates**

## 1. Introduction

Pursuant to the State Administrative Procedure Act Notice in the *New York State Register* (vol. XLIV, issue 21, dated May 25, 2022), Mission:data Coalition, Inc. ("Mission:data") hereby submits this Response to the Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates that was filed May 3, 2022 in the above-referenced dockets (the "Petition"). Below, Mission:data argues that the Petition should be rejected because the proposed Governance Committee is (1) procedurally inappropriate, depriving Energy Services Entities ("ESEs") of due process rights before the Commission; (2) indecipherable and unworkable; and (3) unprecedented across the United States. As for the Self-Attestation ("SA"), while some of the proposed modifications are in theory acceptable to Mission:data, the Petition should nonetheless be rejected because the Joint Utilities have provided no evidence that the Commission's *Order*

*Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings*[1] is inadequate in any way. Finally, the Petition is misguided and administratively inefficient because the Commission's objectives of securing customer data can be more productively reached by addressing the root of the matter – that is, utility liability for an ESE's breach – in a clear and definitive manner, rather than accepting a process of endless cybersecurity updates that must be adjudicated on a monthly or quarterly basis into perpetuity. Until the Commission conclusively removes liability from the Joint Utilities with respect to breach caused by a customer-authorized third party – a policy choice that has been made by numerous other states, as shown in Attachment 1 – the Commission will face unending requests from the Joint Utilities to increase cybersecurity requirements, even if such cybersecurity requirements are unreasonable, costly, impractical or ineffective.

By way of background, Mission:data is a non-profit coalition supporting the rights of consumers to easily and electronically share their energy usage, account and billing information with third parties of the consumer's choice. We have been the leading advocate for the adoption of Green Button Connect ("GBC") over the past decade. Nationwide, GBC has now been required by six (6) states covering over 37 million meters, including in New York. Our members and supporters represent the most advanced distributed energy resources ("DERs") that use customer energy data held by utilities in order to provide tailored energy efficiency, demand response, rooftop solar, and other services. Our members currently play key roles as users of the utilities' existing GBC systems and will be the leading users of the Integrated Energy Data Resource ("IEDR") once the IEDR is available.

## 2. Response

Separate from the merit of the proposed changes to the SA, the Petition should be rejected solely on the basis that its proposal is procedurally flawed and inappropriate. The Petition seeks to establish a Governance Committee with considerable power to establish new

[1] Cases 18-M-0376 et al., Proceeding on the Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, *Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings* (issued October 17, 2019) (the "Minimum Protections Order").

data cybersecurity requirements to which ESEs must adhere. The powers with which the Governance Committee would be vested are tremendous and would undermine both the Commission's authority as well as ESEs' due process rights before the Commission. For these reasons alone, the Petition should be denied.

The proposed powers of the Governance Committee are far-reaching in scope. For example, the Governance Committee – which consists of up to five Joint Utilities members and five Department of Public Service ("DPS") Staff members[2] – would be empowered to "*provide oversight* of New York energy data access initiatives involving cyber security and data privacy risk to ensure necessary protections for entities with access to confidential customer and utility information";[3] regularly update the SA;[4] address "gaps" in Staff's Data Access Framework ("DAF") Cybersecurity Matrix that "require the creation or modification of cybersecurity and privacy protections and processes";[5] determine which ESEs should have their access to customer data revoked;[6] and be the exclusive "deciding group" for all future cybersecurity recommendations.[7] These powers touch virtually all aspects of the requirements with which ESEs' must comply in order to receive customer data with customer permission. Although the Petition states that the Governance Committee will only issue "recommendations" for approval by the Commission, this provides Mission:data with little comfort, given that the Petition demands that the Commission must "act" on the Governance Committee's recommendations within four (4) months of recommendations being issued. Rather than accept established law, rules and norms of practice and procedure before the Commission, the Joint Utilities demand a shortcut – a quick "up or down" vote by the Commission, within four months – with little justification. 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'

---

[2] Petition at Appendix B, page 2.

[3] Petition at Appendix B, page 3.

[4] Petition at Appendix B, page 1.

[5] *Id*.

[6] Petition at Appendix B, page 2.

[7] Petition at Appendix B, page 3.

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

In attempting to justify their sweeping proposal, the Joint Utilities inadvertently illustrate why dissenting views are necessary. For example, the Petition asks that the SA be modified to state, "Authentication and password controls [must] align with NIST 800-63B: Digital Identity Guidelines." At first, this proposal might appear innocuous: Who would oppose helpful guidelines published by a respected federal agency? Surely such guidelines would only help, and not hurt, New York ratepayers. However, upon closer inspection, it becomes clear that granting the Petition would be akin to entering an M.C. Escher painting – pleasing to the eye but impossible to construct to practice. This is because NIST 800-63B defines three (3) distinct and conflicting authentication assurance levels for ESE information systems: (1) a simple username and password; (2) a two-factor or "multi-factor" authentication, typically achieved with a username and password and another device, such as a smartphone, through which an unencrypted one-time passcode is transmitted; and (3) multi-factor authentication with an encrypted key available through, for example, a smartphone application such as Microsoft Authenticator. After inspecting the text of NIST 800-63B, one must ask: With which of these distinct assurance levels must ESEs comply? The Petition does not say. Is it possible for an ESE to be in compliance with all three methods at the same time? No, because there are internal conflicts: to comply with Authentication Assurance Level #1 is to violate Levels #2 and #3; to comply with Authentication Assurance Level #2 is to violate #1 and #3; and to comply with Authentication Assurance Level #3 is to violate #1 and #2.

The Petition does not reckon with its own edicts. By substituting pleasing-sounding federal acronyms and undefined "guidelines" for concrete technical requirements, the Petition discards intelligibility. In order to ratify any policy, Mission:data believes the Commission must first be able to read the standards proposed by a petitioner. In this case, reading NIST 800-63B does not lead to decipherable requirements. In fact, reading the NIST standard in question leads to internal conflicts and metaphysical questions, such as: how can an ESE simultaneously provide an encrypted ***and*** an unencrypted two-factor code in order for an ESE employee to login

to a computer system that stores customer data? Perhaps the only way to comply with such a requirement is to enter quantum physics, the only realm Mission:data is aware of in which matter can exist in two different states at the same time.

To be clear, Mission:data is not resisting a rational discussion of cybersecurity requirements. The Commission has made clear that customer privacy and security are important, and Mission:data welcomes the opportunity to engage with the Joint Utilities and the Commission on whether modifications to prior Commission orders are, in fact, warranted. But the Petition is indecipherable and unworkable in its current form. In addition to the aforementioned standard, NIST 800-63B, regarding digital identity, the Petition also requires encryption of customer data in transit using "encryption methods compliant with NIST cryptographic standards and guidelines." What are these "standards" and "guidelines" regarding encryption methods? We do not know. By our count, NIST has published "standards" and "guidelines" covering at least twelve (12) distinct cryptographic approaches, including: block cipher techniques; digital signatures; hash functions; interoperable randomness beacons; key management; lightweight cryptography; message authentication codes; multi-party threshold cryptography; post-quantum cryptography; privacy-enhancing cryptography; random bit generation; and elliptic curve cryptography.[8] Within these categories are numerous other options left unspecified by the Petition, each conflicting with the others, such as: how many bits are to be used in the cipher (128-bit, 256-bit or 512-bit); whether public keys or private keys are to be used; and acceptable levels of randomness or "collisions" in key generation. Moreover, the Petition's requirement for encryption in transmit would add confusion for our members who have implemented Green Button Connect, which requires a type of encryption known as Transport Layer Security v1.2. If our members are being asked to comply with a different encryption regime, GBC would be rendered functionally inoperable. The Petition does not say what it means. But neither can the Petition mean what it says because of conflicts with pre-existing Commission-approved data access methods. Each proposed "standard" and "guideline" in the Petition confuses, rather than enhances, the requirements to which ESEs must comply.

In addition to being indecipherable and unworkable, the Petition increases the threat of discriminatory treatment of ESEs. When compliance with cybersecurity requirements cannot be

[8] See, e.g., https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

objectively determined as a result of poorly constructed language, the Joint Utilities would acquire the power to subjectively judge ESE compliance at their whim. After all, ESEs could simultaneously be in compliance *and* out of compliance with NIST guidelines. While inside a box, Schrödinger's cat exists in a state of being simultaneously dead and alive until the point at which the cat is observed. At the moment of observation – in this case, when a utility decides to allow or deny an ESE's data request – its final state is determined. The Petition allows the Joint Utilities to selectively revoke an ESE's access without inspecting an ESE's cybersecurity preparedness at all because objective reality is no longer a consideration. A utility could thus sideline any ESE for any reason, whether legitimate or not; for example, a utility could revoke access to an ESE because the ESE provides a product or service that diminishes the utility's revenue-generating potential or threatens the utility's strategic posture in the marketplace. Rather than increasing privacy and security, the Petition simply empowers the Joint Utilities to act arbitrarily and capriciously against ESEs.

Finally, the proposed Governance Committee significantly diverges from the practices in other states. As shown in Attachment 1, the Petition would be unprecedented in the United States among jurisdictions with data-sharing requirements for utilities. Whereas the approach taken in all other states is to establish a definitive set of eligibility requirements – that is, requirements that remain largely unchanged over time – the Petition would, if granted, impose an ever-changing panoply of cybersecurity requirements. The business uncertainty caused by this moving target would, in Mission:data's estimation, cause many of the data-dependent DERs in New York to leave the Empire State and operate elsewhere, depriving New York of the entrepreneurs and innovators that will be necessary to achieve the state's aggressive emissions reductions goals. If the Joint Utilities are permitted to issue convoluted and self-conflicting requirements that may be very costly to comply with – and the opportunity to contest such requirements before the Commission is limited – then the Commission should not be surprised to see its data-sharing efforts flounder as ESEs flee New York for other jurisdictions that offer more consistent and predictable policies.

Mission:data concludes our comments with one final thought. In order to avoid the myriad problems and fatal flaws with a Governance Committee that Mission:data has identified, one potential solution would be for the Commission to simply exempt ESEs that receive customer data with the customer's permission from any outcome of the Governance Committee.

If what the Joint Utilities seek is Commission ratification of continuously updating cybersecurity requirements, then Mission:data would support such an idea, so long as the requirements apply only to data obtained *without* customer authorization. In fact, the Petition appears to be amenable to this approach because it cites a 2010 case in which the Commission approved a data-sharing arrangement between Central Hudson and Opower,[9] which did not receive consent of individual customers. In this way, differential treatment between customer-consented data and unconsented data is one possible method for resolving New York's ongoing disputes over data access policies.

## 3. Conclusion

Ultimately, in Mission:data's view, the Petition is "security theatre" – the performance of precautionary gestures that lack underlying substance. The Governance Council is procedurally inappropriate and undermines the Commission's ability to receive dissenting views from ESEs in adversarial proceedings. For the above stated reasons, Mission:data respectfully requests that the Petition be denied.

Respectfully submitted this 22nd day of July, 2022.

_____/s/_____
Michael Murray, President
Mission:data Coalition
1752 NW Market Street #1513
Seattle, WA 98107
Tel: (510) 910-2281
Email: michael@missiondata.io

[9] Petition at 3.

## Attachment 1

**Comparison Table of Data Access Policies Enacted**

| | *California* | *Colorado* | *Illinois* | *New York* | *Texas* |
|---|---|---|---|---|---|
| *Date that utility I.T. systems were implemented for third party use* | *2016* | *2021* | *2018* | *2019 (ConEd)* | *2016* |
| **Policy Attribute:** | | | | | |
| Utility liability for a third party's misuse of customer data | No liability | No liability | No liability | Liable | No liability |
| Simple third party eligibility criteria established by the Commission | Provide contact info, agree to privacy terms, must not be on the Commission-maintained list of "banned" third parties | None. Rule 3027(e) says, "Nothing in these rules shall limit a customer's right to provide his or her customer data to anyone." | Must comply with applicable tariff | DSA/SA | Must agree to SMT terms and conditions |
| Cybersecurity requirements of third parties | "Reasonable administrative, technical, and physical safeguards" | No cybersecurity requirements | No cybersecurity requirements | Continuous changes proposed in Petition | No cybersecurity requirements |