ADVANCED ENERGY ECONOMY
Transforming Policy. Expanding Markets.

ACE NY
ALLIANCE FOR CLEAN ENERGY NEW YORK, INC.

advanced energy management alliance

August 9, 2021

VIA ELECTRONIC FILING

Hon. Michelle Phillips
Secretary to the Commission
New York State Public Service Commission
Empire State Plaza, Agency Building 3
Albany, New York 12223-1350

Re: Case 20-M-0082 – Proceeding on Motion of the Commission Regarding the Strategic Use of Energy Data

Dear Secretary Phillips:

Advanced Energy Economy (AEE), on behalf of the Alliance for Clean Energy New York (ACE NY) and the Advanced Energy Management Alliance (AEMA), submits for filing comments in response to the *Petition for Rehearing of Mission:data Coalition* and the Commission's June 9th Notice Concerning Petitions for Rehearing. AEE initially submitted these comments on May 28, 2021, and is resubmitting an identical version now because the initial submission was well before the official comment period began.

Respectfully Submitted,

Daniel Waggoner
Director
Advanced Energy Economy

Comments on Petition for Rehearing of Mission:data Coalition (20-M-0082)

Advanced Energy Economy
Alliance for Clean Energy New York
Advanced Energy Management Alliance

Advanced Energy Economy,[1] the Alliance for Clean Energy New York,[2] and the Advanced Energy Management Alliance[3] (collectively "advanced energy companies") write in response to select issues raised in the *Petition for Rehearing of Mission:data Coalitio*n ("Petition for Rehearing") on the Commission's *Order Adopting a Data Access Framework and Establishing Further Process* ("Framework Order"). Advanced energy companies support efforts to ensure robust and appropriate cybersecurity requirements are in place to protect customer and system data. Such protections can help build confidence in the market for distributed energy resources (DER) and energy-related services and avoid industry-wide impacts from bad actors. They are also necessary to protect critical infrastructure and safeguard public welfare. As noted below, the Commission has worked to balance those protections with access to data through a largely risk-based approach[4] that aligns the risk associated with the data to the required cybersecurity control measure.

[1] AEE is a national business association representing leading companies in the advanced energy industry. AEE supports a broad portfolio of technologies, products, and services that enhance U.S. competitiveness and economic growth through an efficient, high-performing energy system that is clean, secure, and affordable.

[2] ACE NY's mission is to promote the use of clean, renewable electricity technologies and energy efficiency in New York State, in order to increase energy diversity and security, boost economic development, improve public health, and reduce air pollution.

[3] AEMA is an alliance of providers and supporters of distributed energy resources united to overcome barriers to nationwide use of distributed energy resources, including demand response and advanced energy management, for an environmentally preferable and more reliable grid. We advocate for policies that empower and compensate customers to manage their energy usage to make the electric grid more efficient, more reliable, more environmentally friendly, and less expensive. These comments do not necessarily reflect the views of all AEMA members.

[4] In the Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings (Proceeding 18-M-0376, Oct 17, 2019), the Commission established a partial risk-based approach and said that the implementation of a fully risk-based approach required more analysis of applicable cybersecurity and data privacy frameworks. The Commission did not universally require cybersecurity protections and established them only for those ESE's that receive or exchange data from a direct connection with utility IT systems.

We support this risk-based approach to cybersecurity[5] and request that the Commission clarify that a risk-based approach extends to audit requirements as well.

Unlike the interpretation provided in the Petition for Rehearing, we did not read the Framework Order as requiring a SOCII Type 2 audit. The Framework Order stated that a recognized independent audit, such as a SOCII Type 2 audit, could serve in place of the need for the Commission's Cybersecurity Provider ("Provider") to conduct an audit, but did not specify what type of audit the Provider should conduct if one is needed.[6] We are concerned that because the SOCII Type 2 audit was the only type of audit listed in the Framework Order, the Provider might apply it as a general requirement for all forms of data access. A SOCII Type 2 audit is a stringent industry standard and requires substantial time, effort, and expense. If the Provider were to require a SOCII Type 2 audit for an Energy Service Entity (ESE) to access customer usage data, it would likely prohibit all but the largest companies from offering services to customers.

Instead, we request that the Commission affirm that a risk-based approach, which the Commission has largely implemented for cybersecurity requirements,[7] also guides the level of audit that is required for an ESE. We believe a risk-based approach would match an appropriate level of audit with a type of data access, based on the risk associated with the data and transmission method. To ensure a risk-based approach, we ask that the Commission further clarify the audit requirements by adopting the following parameters:

- A SOCII Type 2 audit should not be a universal requirement. We understand that the Commission has not required this audit type, but it may be interpreted as such since it was the only audit type that was specifically referenced in the Framework Order. The Provider may deem it appropriate to require a thorough audit to make sure the highest security protocols are in place for certain purposes, such as two-way operational data transferred between and ESE and the utility, but a SOCII Type 2 audit should not be a default.

- Audit requirements should be low for customer data accessed through a secure portal. Downloads of customer usage data through a secure portal, such as via Green Button Connect, pose very low risk for several reasons. These portals are segregated from utility operational systems and provide one-way data transfer from the utility to the ESE. Customer usage data is mainly a privacy concern, and while customer privacy is an important issue, there are levels of security lower than a SOCII

[5] Comments of Advanced Energy Economy, Alliance for Clean Energy New York, and the Advanced Energy management Alliance on Joint Utility Petition for Authority to Enforce Data Security Agreements, Proceeding 18-M-0376, filed April 30, 2019, p 6.

[6] Framework Order at 16

[7] See supra note 4

audit that are sufficient to protect it. Also, usage data is generally not of value to anyone else except for other ESEs. It is of much less interest than say payment information, which is already protected by state and federal laws and significant corporate liability if a breach occurs.

- Access to anonymized or aggregated usage data should not require an audit. There are no security concerns associated with the release of anonymized or aggregated data, nor are there privacy concerns. Advanced energy companies are unable to find any risks associated with the release of this type of data, and therefore believe access to it should be exempted from audit requirements.

- Audits should ensure stringent cybersecurity protocols are in place for data exchange with utility operational systems or access to data with security implications. Given the frequency and increasing impact of cybersecurity breaches, we support measures that mitigate the threat to utility systems by ensuring anyone entrusted with secure system data has strict safeguards in place.

The Commission has spent significant effort in developing ambitious policies for the collection and distribution of energy-related data in New York, and we would like to avoid any misapplication of the audit requirements from creating unnecessary barriers that might hinder the Commission's efforts. At the same time, we fully support robust cybersecurity requirements to ensure that the most sensitive data remains secure. Advanced energy companies support clarifying the audit requirements and extending the existing risk-based approach to accomplish these dual purposes.