April 29, 2019

VIA ELECTRONIC FILING

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

   Case 18-M-0084 – In the Matter of a Comprehensive Energy Efficiency Initiative

Dear Secretary Burgess:

Advanced Energy Economy Institute (AEE Institute), on behalf of Advanced Energy Economy (AEE), the Alliance for Clean Energy New York (ACE NY), the Northeast Clean Energy Council (NECEC), the Advanced Energy Management Alliance (AEMA), and their joint and respective member companies, submit for filing comments on the 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 Execution of the Data Security Agreement by Entities Seeking Access to Utility Customer Data or Utility Systems.

Respectfully Submitted,

Ryan Katofsky
Managing Director
Initial Comments on the Joint Utility Petition for Authority to Enforce Data Security Agreements (Cases 18-M-0376, 15-M-0180, 18-M-0084)

Advanced Energy Economy Institute  
Alliance for Clean Energy New York  
Northeast Clean Energy Council  
Advanced Energy Management Alliance

Preface

In order to prepare comments on the 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 Execution of the Data Security Agreement by Entities Seeking Access to Utility Customer Data or Utility Systems (“Petition”), Advanced Energy Economy Institute (AEE Institute) is working with Advanced Energy Economy (AEE) and two of its state/regional partners, the Alliance for Clean Energy New York (ACE NY) and the Northeast Clean Energy Council (NECEC), as well as Advanced Energy Management Alliance (AEMA),¹ and their joint and respective member companies to craft the comments below. These organizations and companies are referred to collectively in these comments as the “advanced energy companies,” “we,” or “our.”

Summary

Advanced energy companies support efforts across the energy sector to strengthen cybersecurity. As providers of technologies and services both to end-use-customers and utilities, advanced energy

¹ AEE is a national business association representing leaders 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. 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. NECEC is a regional non-profit organization representing clean energy companies and entrepreneurs throughout New England and the Northeast. Its mission is to accelerate the region’s clean energy economy to global leadership by building an active community of stakeholders and a world-class cluster of clean energy companies. 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.
companies face cybersecurity threats from multiple angles, and are keenly aware of the importance of protecting customer data. We support the Commission’s efforts to increase cybersecurity protections. We also want to ensure that these efforts are directed toward the most critical interactions and that they provide security without imposing unnecessary costs or preventing further animation of the distributed energy resources (DER) market in New York.

Our primary concern with the Petition and the Data Security Agreement (DSA), which the Joint Utilities of New York (JU) seek authority to enforce, is the broad strokes used to address diverse types of data transactions. Not all forms of data and all methods of exchange pose the same level or risk, though the DSA makes no distinction and treats all of them the same. Further, the DSAs cover multiple types of entities, such as Energy Service Companies (ESCOs), DER Suppliers, and third parties; however, the rationale applied to the requirements in the DSA is based on a vendor relationship between a company and a utility and does not adequately account for a third party’s relationship with its customer.

In addition to the broad applicability of the DSAs, we believe that the business-to-business process that was used for developing the DSA—that the JU seek to affirm—is not appropriate for establishing the terms under which the JU should fulfill a Commission-imposed requirement that the JU in many cases do not benefit from (that is, to provide data to third parties at the customer’s election). In particular, third parties have anti-competitive and market-access concerns that are not likely to be handled well through a business-to-business process. The Commission in its Order Adopting Accelerated Energy Efficiency Targets specifically called for a separate process to address the terms and conditions for accessing Green Button Connect. The Commission stated:

The utilities and Staff are directed to conduct a collaborative with DER providers and other interested parties to develop GBC terms and conditions that are consistent across utility service territories. The terms and conditions should make it no more difficult for a DER provider, for whom a customer has provided consent, to access data than it is for the individual customer to access data.

The GBC collaborative is the appropriate place to address issues related to third-party access to customer data, including cybersecurity concerns that are specific to these data exchanges. The business-to-business process is inappropriate for addressing cybersecurity concerns with third parties. Further, the DSA imposes conditions that do make it more difficult for a DER or third-party provider to access a customer’s

2 The use of third party in this document is different from how it is used in the DSA. The DSA uses the term Third Party Representative to mean a vendor or contractor performing services and acting on behalf of an Energy Service Entity. We use third party to refer to any entity that serves a customer on their own behest and not because of a business or contractual relationship with a utility. That is, a utility and a third party both have a common customer, and the third party’s relationship to the customer is independent and distinct from the utility’s relationship to that customer.

data, with the customer’s consent, than it is for the individual customer to access their data. We therefore respectfully recommend that the Commission affirm the GBC collaborative as the venue for addressing GBC data security requirements and direct Staff to lead a separate stakeholder process to revise the DSA under certain guidelines (proposed below) to address non-GBC data exchanges and then adopt a final DSA following stakeholder comment.

Discussion

The Petition Does Not Distinguish Between Different Customer, Utility, and Third-Party Relationships

We understand the JU’s desire to ensure adequate cybersecurity measures are in place to safeguard customer and system data. This is an important concern when the utility relies on an outside vendor to perform a service on its behalf and under its own name. In these situations, the utility has reputational and operational concerns and may also be at risk for liability. It is this sort of vendor relationship that the petition chiefly relies on. If this Petition were limited to affirming the authority of utilities to establish cybersecurity requirements for their vendors or other direct business partners, we would not object.

However, the applicability of the DSA is not limited to vendors. The DSA also applies to Energy Service Entities (ESEs), which are broadly defined in the DSA as follows:

“ESE” shall have the meaning set forth in the Recitals and for the avoidance of doubt, includes but is not limited to ESCOs, Direct Customers, DERS and contractors of such entities with which Utility electronically exchanges data other than by email and any other entities with which Utility electronically exchanges data other than by email or by a publicly available portal.4 [Bolding added for emphasis]

This makes clear that the DSA is meant to cover more than vendors and other companies with a direct business relationship with a utility. It would also include third parties that have no direct business relationship with the utility and are instead offering services directly to their own customers. The customer may wish to share their data with the third party directly via the utility using a protocol such as Green Button Connect. This sharing of data does not confer a business relationship between the third party and the utility. Instead, it is access that extends from the customer’s right to their own data and their ability to provide it to other parties that they designate.

Despite this important distinction between vendors and third parties, the Petition relies on prior Commission decisions for data requirements for vendors and makes no distinction between vendors and third-party providers. In the Petition, the JU states that “ESEs should be treated as any other vendor.”

---

4 Data Security Agreement, p. 3
Further the Petition states that “the Joint Utilities do not contract with vendors that do not meet their required cyber security terms. Yet, the ESEs have not demonstrated any reason that they should receive different treatment.” This argument does not recognize the very important distinction that third parties are acting at the customer’s behest to access data they have a right to and not as part of a transaction or business arrangement with the utility. The mere election of the customer to share their own data with the third party does not create a business relationship between the third party and the utility.

The JU Petition, if approved by the Commission, would improperly create multiple obligations for a third party toward a utility, such as audit requirements, insurance, and indemnification of purported liability to the utility. Third parties are liable for breaches of data security and confidentiality and should bear the costs of safeguarding their systems and providing restitution to their customers if breaches occur; however, they are liable to their customers for securing their data and not to the utility. As we discuss later, the one-way transfer of historical usage data from the utility to a third party poses no more security or operational risks to the utility than when a customer directly downloads their data from a utility portal.

The Petition also does not account for the fact that customers often direct another person or company to act as an agent on their behalf with a utility. The legal concept of agency is well-established in Federal Law and the laws of New York State. Customers may designate an agent for many reasons. The reasons may be for commercial purposes, such as managing usage and billing across multiple accounts, or other reasons, such as care giving and providing judges with a means to ensure utility bills are paid and properties are maintained during property disputes or divorce. Agents should be allowed to fully interact with the utility with the same access as the customer/principal that designates the agent.

**The Petition Does Not Adequately Account for the Rights of the Customer**

Customers have a right to access all of their data, including billing, account, and usage information, and the Commission has affirmed that customers must be able to access their own billing determinants at the granularity that is used for their particular tariff. Customers also have a right to conduct business with third-party providers, many of whom have no interaction with utility systems and the furnishing of electricity. Many third-party products fall under the category of general consumer goods unrelated to the furnishing of electricity (e.g., thermostats) that help manage the customer’s consumption of energy for the customer’s benefit.

---

5 Order Adopting a Ratemaking and Utility Revenue Model Policy Framework, Case 14-M-0101, Page 142

6 Within the Track 1 Order (14-M-0101), the Commission stated that Public Service Law Sec 2(12) limited its oversight to DER Provers only when their services are furnishing electricity, or contributing materially to core DSP functions that are furnishing electricity.
We do not claim that the Commission has no authority to set requirements for the utility’s distribution of data to other parties. However, it is doubtful that the Commission would have authority to regulate the ability of a customer to download their data and provide it directly to a third party that has no business relationship to a regulated utility (and further, is not supporting the furnishing of electricity). If the Petition is granted, both third parties and customers would face a stark difference in the cost of the method through which the third party accesses the customer’s data. A direct transfer from the customer would cost little, while receiving the data from a utility subjects the third party to audit, costly insurance requirements, and additional utility control of the customer’s data. Customers would also face the hassle of obtaining and transferring the data as well as greater security risks since it would involve the customer’s own computer or IT systems—a potential weak link.

The Commission should be cognizant that a direct transfer of data from the customer remains an alternative if the conditions of the DSA prove to be overly restrictive or too costly. However, it is far from an ideal solution. Customers will have to live with the hassle of providing the data, and where third parties require periodic data updates to perform the services they contract with customers to provide, there is risk that the hassle may outweigh the benefits the customers experience and lead to customer attrition. Third parties will have concerns about the authenticity and timeliness of the data, and in cases where the data is used for validation of another metric to another entity, data provided in this manner may not meet these requirements. Third parties may avoid New York as a market if the cost of obtaining data is prohibitive, limiting customer choices and the benefits of services that customers otherwise would have enjoyed.

We are also concerned with the inclusion of Direct Customers in the DSA’s definition of ESE and the applicability of the DSA to them. Direct Customers receive only distribution service from the utility and procure supply directly from the NYISO. Direct Customers exchange data with the utility through the EDI, and because of this, may pose different data security concerns than a typical retail customer. Two-way data flows between the utility and customer pose a greater cybersecurity concerns than one-way downloads, and if Direct Customers engage in two-way data exchange with the utility via the EDI, utilities may have legitimate cybersecurity concerns. Because a two-way data transfer is distinct and raises different concerns from a one-way transfer of customer usage data, it should be covered under a separate DSA that is tailored to those concerns. Regardless, any data security requirements must be balanced with the fact that Direct Customers are utility customers and have a right to access their data. The requirement that Direct Customers take out cybersecurity insurance policies to indemnify the utility against damages creates a high cost for accessing their own data.

\[\text{7 For example, if an energy efficiency measure is installed and data analysis provided by a third party is required to validate that the measure has achieved its desired result, or if a customer participates in a demand response program and the data does not meet the program administrator’s requirements for data management practices.}\]
The Petition Does Not Recognize that Different Types of Data Access Pose Different Levels of Risk

Granting this Petition would create a blanket requirement that all types of data exchanges be covered by a DSA, even if the type of data exchange in question poses no risk to the utility. The DSA only makes an exception for data transmitted “by e-mail or by a publicly available portal.” However, there are different levels of risk to the utility based on the type of data in question and the method of its transmittal. If the utility provides sensitive data about critical equipment to a party, it has a responsibility to enforce the confidentiality of that system data to protect itself and its customers. In situations where the utility receives operational data from ESEs, such as for real-time generation from a DER participating in a Non-Wires Alternative, the reliable provision of energy to customers relies on the security of this data exchange. Further, two-way data exchanges also grant a higher degree of access to utility systems and increase cybersecurity concerns.

For one-way transfers of non-operational data, such as a customer’s historical usage, the risk to the utility is extremely low. An example of this is a customer downloading their data via Green Button. Residential utility customers are not required to execute DSAs with the utilities, despite the high likelihood that many of their computers may be infested with malware and other cyber threats. This is because there is no threat to utility systems from this one-way data exchange. The process for Green Button Connect is the same, except that there is an additional authorization step to ensure that the customer agrees to this data transfer. The risk to the utility of the one-way data transfer to a third party is the same as a transfer between the utility and its residential customer. An analogy would be to consider the threat to the utility if a customer gave a stack of paper utility bills to a third party that were then subsequently stolen from the third party. The third party would be liable to their customer for the theft of their personal data, but the threat to the utility is non-existent. Green Button data would have even fewer personal confidentiality concerns than a mailed utility bill as Green Button standards prohibit the inclusion of personally identifiable information (PII).

Given the lack of risk to the utility for a one-way transfer of customer usage data, the Petition, were it to be granted, would impose unjust costs on third parties to require them to indemnify the utility with $5 million in insurance coverage as a prerequisite to accessing their customers’ data. The JU’s argument for requiring insurance relies on the potential for shifting costs from ESEs to utility customers if a data breach results in damages to the utility that the ESE cannot pay for. But if the utility is not at risk from a one-way

---

8 Data Security Agreement, p. 3
9 See http://www.greenbuttondata.org/residential.html
The transfer of customer data to a third party, then the insurance requirement is unjustly imposing an entirely artificial cost on third parties and their customers.

**The Business-to-Business Process is an Improper Means for Establishing Requirements on Entities without a Business Relationship with the Utility**

The JU Petition is seeking the Commission’s affirmation of the business-to-business process through which the DSA has been developed. For transactions between parties where each stands to benefit from their business relationship and each willingly negotiates on a level playing field, we would normally endorse a business-to-business process rather than seek the Commission’s intervention because it allows for greater flexibility in contracting and lowers transaction costs. However, these are not the circumstances under which this business-to-business process is being conducted.

In many cases, the utility’s only interaction with a third party will be a data transfer. The third party, acting at its customer’s direction, is seeking its customer’s data from the utility rather than negotiating the terms of sale for a service that the utility stands to benefit from. The utility may not stand to benefit from this transfer of data and may negotiate with the intention of establishing barriers to the release of data rather than entering the process as a willing participant. Since the Commission ultimately required utilities to provide customer data to third parties at the customer’s direction, the Commission should also be involved in deciding the terms under which that data is provided to ensure that the terms do not create artificial barriers to customers exercising their rights to use their own data as they choose.

Given the foregoing, we recommend that the Commission affirm that the GBC collaborative is the appropriate venue to address cyber security requirements for third parties using GBC. We also recommend that Staff redraft a DSA applicable to non-GBC exchanges through a new Staff-led stakeholder process that results in a recommendation that is open to comment from parties before the Commission ultimately establishes a DSA. This DSA should not be open to unilateral modification by the utilities as requested in the Petition. In order to ensure that the DSA appropriately handles each type of data exchange, we recommend that the Commission include the following guidelines for the development of a new DSA:

1. The DSA should recognize the different types of relationships between customers, vendors, third parties, and utilities. Utilities should have greater discretion in deciding the terms under which they provide data to parties as part of business transactions while there should be greater protections for third parties in their engagement with utilities, as there are concerns over anti-competitive practices and market access.

2. The DSA should not treat all forms of data equally. Different types of data carry different levels of risk, and the rights of the customer to their own data should guide decision making.
Utilities should have some bounded discretion over whether and how it provides its own data to outside parties, especially when that data is sensitive and its release could pose security concerns. The ownership of customer data should reside with the customer and utilities should have a perpetual right to store and use this data to plan for and operate their systems. If the customer elects to provide access to their own data to a third party, the requirements for the release of data to the third party should be minimal.

3. The DSA should not treat all types of data exchange equally. The method of transfer of the data, whether the data flow is one- or two-way, and the relationship of the utility system being accessed to sensitive utility operations should be considered. One-way downloads of data from customer-facing systems, two-way transfers of data through the EDI, and two-way transfers of data through utility operational systems carry different levels of risk and should be treated distinctly.

**Conclusion**

Data access is a critical issue for an animated market for consumer energy services of all types. For several years now, New York State policy has been focused on growing an animated market for energy efficiency, demand response, and other distributed energy resources and transforming the market so that natural market forces can help grow these customer-driven investments beyond state-supported programs. Most of these customer-driven transactions will be with third parties. New York’s efforts to promote innovation and grow this market will be hamstrung without low-cost and easy access to data. This does not mean that the market should develop without accounting for the cost of keeping customer data secure and restitution for customers when breaches occur. However, as written, the DSA creates artificial costs for some types data exchanges because it treats all types of data, different means of exchange, and types of relationships with outside parties as the same.

Well-intentioned efforts to protect customers data that are overly restrictive and limit customer choice are not cost free. We encourage the Commission to find the appropriate balance, as cybersecurity requirements that are not appropriately focused will impair the productive use of energy data, limit the potential for vibrant markets for energy services, and ultimately impede private consumer investment that will help meet the state’s important greenhouse gas reduction goals.