Consumer Power Advocates

Columbia University Medical Center
Fordham University
Memorial Sloan Kettering Cancer Center
Mount Sinai Health System
New York Presbyterian Hospital
New York University
NYU Langone Medical Center

December 14, 2018

VIA ELECTRONIC FILING

Honorable Kathleen H. Burgess
Secretary
New York Public Service Commission
Three Empire State Plaza
Albany, New York 12223-1350

RE: Case 18-M-0376 – Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place.

Dear Secretary Burgess,

On November 14, 2018 the Commission convened a meeting of the stakeholders in the above-captioned proceeding (Stakeholder Meeting.) Pursuant to request made by department staff in that meeting, the Consumer Power Advocates (CPA) and Luthin Associates, Inc. (Luthin) hereby submits their written summary of the concerns they raised during the meeting. The Stakeholder Meeting was, in part, occasioned by the request for a declaratory ruling by the Joint Utilities confirming that a distribution utility may discontinue an energy service company's participation in the utility's retail access program pursuant to Section 2.F. of the Uniform Business Practices (UBP) for failure to meet minimum data security standards and numerous responses thereto by ESCO representatives and others[1].

Consumer Power Advocates (CPA) is a coalition of not-for-profit commercial health care and educational customers in the Consolidated Edison (ConEd or the Company) service territory that advocates on behalf of consumer interests before the Commission, NYISO and elsewhere.

[1] / Case 18-M-0376, Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, Petition of the Joint Utilities for Declaratory Ruling Regarding Their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices (filed November 9, 2018) (JU Petition).

535 Main Street, Allenhurst, NJ 07711
Tel 732-774-0005 Fax 732-774-0049

Luthin Associates is an energy consultancy that represents CPA, and provides various energy services, including energy procurement and management, to end-users in New York City. Both Luthin and CPA members routinely interact with the Company's computer systems to obtain customer usage data. As such, both are implicated by the issues being discussed in this proceeding.

## Applicability and Awareness

CPA and Luthin (hereafter, "we") initially note that while ConEd has made it quite clear that it believes that the requirements outlined in its proposed Data Security Agreement (DSA) and Self-Attestation Form (SAF) are intended to apply to retailer/energy service companies (ESCOs,) Distributed Energy Resources (DERs,) as well Energy Service Entities (ESEs.) The latter of these constitutes an entirely new group of entities, the definition of which is very loose, but which appears to include essentially any entity that interacts directly with the Company's computer systems to obtain customer data[2]. The requirements imposed on these entities are also intended to apply to any third-party entity, such as a contractor that does business with them.

Subsequently, in response to a petition by the Retail Choice Coalition[3], the Secretary issued a Notice extending the comment deadline and clarifying the applicability and scope of the JU Petition. Specifically, with respect to the latter, the Secretary noted that

> The JU Petition seeks interpretation of UBP §2.F., which applies only to ESCOs, and any discontinuance undertaken could only be taken against an ESCO. While it is correct that similar cyber security issues are being addressed with respect to DER providers, there is a separate process being undertaken for those entities, and an interpretation of the discontinuance provisions of the UBP for ESCOs does not necessarily implicate any similar requirements imposed upon DER providers[4].

The Stakeholder Meeting was an important part of that "separate process" and we are

[2] / At the Stakeholder Meeting, ConEd's attorney provided a succinct summary of those to whom the requirements are intended to apply: "Anyone who touches our systems." Subsequently, she clarified that they should also apply to "anyone who touches the systems of anyone who touches our systems." Asked whether they should also apply to the next and further layers down, ConEd did not confirm that there was any level of removal from the Company's systems beyond which it would be comfortable with the requirements not applying.

[3] / Case 18-M-0376 Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, Request of the New York Retail Choice Coalition and Supporting ESEs For An Extension Of Time To File Comments On Petition Until Expiration Of 60 Day Comment Period Under State Administrative Procedure Act And, In The Alternative, Requests the Secretary to Require Service to All Interested Parties, and a Three Week Extension to Submit Comments (Coalition Request,) New York Retail Choice Coalition (Coalition) (filed November 27, 2018)

[4] / Case 18-M-0376 Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, Notice Extending Comment Deadline, Issued November 30, 2018, at 3.

hopeful that our comments here can result in an appropriate, workable outcome that provides reasonable cyber protections while not erecting such barriers to participation that DERs, ESEs, and third parties cannot afford to enter, or are driven out of the market.

Initially, we note that whatever the process was that led to the version of the DSA and SFA that are the subject of the JU Petition, and that the JU believe should apply to DERs, ESEs and third-parties, the general body of DERs and third-parties were not active participants in it. Indeed, it is certain that nearly all of the potentially affected third party contractors to ESCOs, DERs and ESEs are unaware of this proceeding and ignorant of the fact that their ability to do business in New York State is under threat. Even following the Stakeholder Meeting, it is not clear that all, or even most, DERs are aware that potentially onerous and expensive cybersecurity rules are being developed for them. The Secretary's action to serve her Notice on participants in the DER Oversight and Comprehensive Energy Efficiency dockets is helpful, but likely still misses some DER firms and definitely misses many firms in the ecosystem of third-party contractors. If appropriate due process protections are to be provided, the Commission, the utilities, ESCOs, DERs and others involved in the proceeding to date need to do more to ensure that potentially affected parties are aware of that fact.

Apart from the need to improve the level of awareness of the ongoing process, it is our position that what has gone before with respect to cybersecurity for ESCOs is in no way dispositive of what should apply to DERs or third parties. This view, that ESCO cyber rules do not automatically apply to other entities is confirmed by the Secretary's Notice. Accordingly, we reject any assertion that we are under any obligation at this time to sign the DSA or submit the SAF[5].

There are numerous ways in which these entities and the risks they pose to utilities may be significantly different and thus warrant different treatment. Not least of these differences is the fact that the ESCO industry is large, well-established and sophisticated, and most of its members similarly so. The DER industry, in contrast, is much smaller and newer, consisting of smaller and newer participants. It is not possibly to easily characterize the poorly defined group of "third parties," however, many contractors and consultancies are small and ill-prepared to meet, without undue hardship, all of the same requirements that may apply to large ESCOs.

[5] / Luthin has been told that its access to certain Company systems may be rescinded in the event that we do not execute the DSA or submit the SAF. Luthin rejects the validity of such a requirement unless and until the Commission specifically affirms its validity.

## Self-Attestation Form

We have reviewed the proposed SAF and do not believe that any of the requirements are unreasonable. Given the importance of cyber risk management, sizable firms, such as CPA members already have policies in place to implement best practices, such as those laid out in the SAF. Luthin is a relatively small firm, but our work with NYSERDA and other entities has required us to develop and implement a robust cybersecurity policy. Accordingly, Luthin either already meets or is in the process of implementing each of the SAF requirements with respect to customer data received from the Company, or other data labeled by the Company as confidential.

## Data Security Agreement

During the Stakeholder Meeting, we identified three primary issues with the proposed DSA, each of which is addressed below.

Who is Affected?

The DSA purports to apply to directly ESEs. In turn, ESEs include, but are not limited to ESCOs, Direct Customers, DERs, and contractors to 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." (emphasis added.) In other words, the requirements embodied in the DSA are intended to apply to *any entity* "with which Utility electronically exchanges data other than by email.[6]"

In addition, the DSA requires that every affected ESE must require any third-party entity with which it does business to electronically exchange (other than by email) confidential data not only abide by the requirements of the DSA, but of the Uniform Business Practices (UBO) or Uniform Business Practices – Distributed Energy Resource Supplier (UBP-DERS) as well[7]. ESEs must require all other third-parties to whom access of confidential information would be supplied to agree to the same DSA terms[8].

In short, the DSA would, by its express terms, bind, or require the binding of, the ESE who obtains confidential data from the utility, any intermediary entity is uses to obtain that data,

[6] / Proposed Data Security Agreement dated August 18, 2018 at 3.
[7] / Id at 5.
[8] / Id at 6.

and any entity the ESE might contract with to process that data. Less clearly, but certainly implied by statements at the Stakeholder Meeting, the DSA is also intended to apply to entities beyond third parties who may be retained to process it. It appears that the intent of the DSA is for liability for disclosure by these "fourth-party" (query: fifth, sixth,….?) entities to flow back up the "chain" to the ESE and all intermediate entities.

We have no objection to the application of the DSA terms to ourselves, but we do object to a requirement that we be responsible for actions of those over whose actions we have no control. It will be a difficult and expensive thing to demand that a potential contractor obtain cyber insurance, submit to a possibly invasive, time-consuming, and expensive information security audit by a utility, agree to assist a utility investigation, possibly at its own expense, or open itself up to unlimited liability.

What Data Must be Protected?

The proposed DSA takes a very expansive view as to what information is deemed to be confidential and must be protected. Given the possible consequences of a failure to properly treat confidential information, it is our position that there be no ambiguity in terms of what is defined as confidential information subject to protection. The data required to be provided to or by the utility pursuant to the UBP or UBP-DERS is fairly clear, as it is specifically called out in the UBPs. However, the DSA also includes the following:

> "any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure[9]"

This is not limited to information related to confidential customer data, nor does it have any nexus to the UBP or UBP-DER. It could be any information market confidential by the utility for any reason or in any context[10].

Affected entities are required to go to significant and expensive lengths to protect against the disclosure of confidential information, as defined in the DSA. The data that should be subject to that protection should be limited to only what is needed. Not every piece of data merits the exact same degree of protection, even if it may not be publicly available.

---

[9] / Id at 2.

[10] / It is ironic that the DSA document itself is marked "CONFIDENTIAL." But for the fact that Luthin is not subject to the DSA and the fact that the DSA is publicly available on the Department's web site, this very filing would be violative.

How Must Data Be Protected/Consequences of Disclosure?

The DSA and associated SAF contains many requirements intended to protect against disclosure, most of which are reasonable. We wish to instead focus on two provisions of the DSA that relate to the consequences of disclosure and mitigating the associated utility risks. Utilities are, understandably, attempting to insulate themselves to the maximum extent they can from the impacts of a disclosure. The problem is that no ESE or third party can possibly absorb the level of risk sought to be transferred in the event of a major data security breach for which they may be partially or fully responsible, yet they effort to allocate that risk to the ESE or third party could keep them out of the market altogether.

1. Cybersecurity Insurance – While $5 million in cyber insurance is preferable to $10 million, neither is likely to make a significant dent in the potential costs associated with a major cyber breach. Any cyber insurance policy that would cover the costs to a utility of a large breach would be completely unaffordable. All the proposed requirement appears to do is erect a barrier to entry by smaller firms. This requirement should be eliminated for DERs, contractors and third parties. Focus should instead be on assuring that all entities have robust policies and practices, such as those in the SAF, in place.
2. Indemnification – Similar to cybersecurity insurance, the requirement that ESEs and third parties "hold Utility, its affiliates, and their respective officers, directors, trustees, shareholders, employees, and agents, harmless from and against any and all loss, cost, damage, or expense of every kind and nature (including, without limitation, penalties imposed by the Commission or other regulatory authority or under any Data Protection Requirements, court costs, expenses, and reasonable attorneys' fees) arising out of, relating to, or resulting from, in whole or in part, the breach or non-compliance with this Agreement by ESE or any of its Third-Party Representatives except to the extent that the loss, cost, damage or expense is caused by the negligence, gross negligence or willful misconduct of Utility" is nonsensical. Any major breach could result in tens or hundreds of millions of dollars in costs, costs that no ESE or third party could possibly pay. In addition, the ways in which arguable non-compliance could occur, even unknown to the ESE or third party, are many. Instead, faced with accepting such liability many entities would instead choose to do business elsewhere.

Requirements Must be Knowable

The DSA imposes a myriad of requirements on ESEs and third parties and there are significant consequences for failing to meet the requirements and maintain compliance[11]. Many of these will be new, even for those parties who have attempted to be diligent about cyber protections. However, even the most sophisticated participants may find some of the requirements nearly impossible to meet.

For example, a breach of "any" Data Protection Requirements would (A) create a Data Security Incident, resulting in the suspension of the ability to do business, possible requirement to erase all customer data and obligation to pay millions of dollars in compensation to the utility[12]. What are the Data Protection Requirements whose breach could have such catastrophic impacts?

a. "Data Protection Requirements" means, collectively, (A) all national, state, and local laws, regulations, or other government standards relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESE or its Representative's Processing of Confidential Utility Information; (B) industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls as best industry practices and frameworks may evolve over time; and (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved UBP and UBP DERS.

We doubt that even the states utilities know, let alone comply with, all "industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls as best industry practices and frameworks may evolve over time[13]." The idea that every entity subject to the DSA would or even could is ridiculous. No entity without staff dedicated to following cyber threats and

[11] / Failure to maintain compliance with most provisions is considered a material breach of the DSA with the relevant utility and result in the denial of the ability to access, process and retain customer data. For many firms, who rely upon this data, this amounts to being put out of business in that utility territory. For a small ESE focused in one area of the state, it amounts to a corporate death sentence.

[12] / DSA Section 8 at 7 and Section 11 at 9.

[13] / DSA at 2.

cybersecurity issues on a full-time basis could hope to understand these requirements, let alone maintain compliance as "they may evolve over time." Section DSA Section 1.d(B) should be deleted in its entirety.

Derivative Data Prohibition

Section 14a of the DSA prohibits the creation or maintenance of data which are derivative of Confidential Utility Information unless it is for the purposes of the DSA or as authorized under the UBP or UBP-DER. This prohibition is unreasonable.

Where a customer has consented to the use of its data for a particular purpose, regardless of whether it is for the purposes of the DSA or authorized under the UBP, the fact that the data was obtained from the utility should be immaterial.

Luthin often develops derivative data and analyses for its clients (including CPA members) using data they have authorized it to obtain from ConEd. It is not reasonable to bar Luthin and other consultants from engaging in analytical work simply because the utility wants to assert proprietary rights over data. The data is the customers', not the utilities', a fact that is not changed by the fact that utilities are the ones that hold it.

## Conclusion

While the SAF appears to be, for the most part, reasonable, the DSA is not. It is a lopsided agreement crafted without the benefit of input from most of those whom the utilities intend that it should apply to that attempts to insulate the utilities to the maximum extent possible from cyber risks, while imposing unreasonable requirements on entities least able to accommodate the compliance burdens. If implemented as proposed, the DSA would discourage new entities from participating, could drive existing participants out of the market, and likely do both without meaningfully reducing the risks of a major cyber breach. A better process is needed that will more appropriately align responsibilities with risks.

CPA and Luthin appreciate the opportunity to provide its views to the Commission and respectfully recommends that they be adopted in any final order the Commission may issue.

Respectfully Submitted,

/s/
Aaron Breidenbaugh
Director of Regulatory Affairs