STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

In the Matter of Retail Access Business Rules	**)**	**Case 98-M-1343**
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	**)**	**Case 18-M-0376**

Response of the
National Energy Marketers Association
To the Petition of the Joint Utilities for Declaratory Ruling
Regarding Their Authority to Discontinue Utility Access to
Energy Services Companies in Violation of the Uniform Business Practices

The National Energy Marketers Association (NEM)[1] hereby respectfully submits this Response to the "Petition of the Joint Utilities for Declaratory Ruling Regarding Their Authority to Discontinue Utility Access to Energy Services Companies in Violation of the Uniform Business Practices" that was filed on November 9, 2018. This Response is filed pursuant to 16 NYCRR 8.2(c). The Joint Utilities (JU) petitioned the Commission "to issue a declaratory ruling confirming the Joint Utilities' right under the UBP to discontinue an Energy Service Company's ("ESCO") access to Petitioners' various systems, in their relevant retail access program, if that ESCO fails to meet minimum data security standards, including the execution of a Data Security Agreement ("DSA") in accordance with UBP provisions governing 'Eligibility Requirements' for ESCOs." (Petition at

[1] The National Energy Marketers Association (NEM) is a non-profit trade association representing both leading suppliers and major consumers of natural gas and electricity as well as energy-related products, services, information and advanced technologies throughout the United States, Canada and the European Union. NEM's membership includes independent power producers, suppliers of distributed generation, energy brokers, power traders, global commodity exchanges and clearing solutions, demand side and load management firms, direct marketing organizations, billing, back office, customer service and related information technology providers. NEM members also include inventors, patent holders, systems integrators, and developers of advanced metering, solar, fuel cell, lighting, and power line technologies. This document reflects the views of NEM and does not necessarily reflect the views of any specific member of the Association. This Response is not intended to serve as a waiver of any rights, arguments, claims or remedies, all of which NEM expressly reserves.

1-2). Not only are the JU claiming the right to discontinue ESCO service, the JU also "believe the UBPs permit individual utilities to initiate the discontinuance process pursuant to UBP Section 2(F)(2) *without intervention of the Commission*." (emphasis added) (Petition at 8).

NEM supports the development and implementation of reasonable cybersecurity standards for the retail energy marketplace. However, the Data Security Agreement (DSA) and Self Attestation (SA), developed through the utilities heavy-handed business-to-business process, still suffer from areas of major substantive disagreement. As such, an ESCO decision not to acquiesce to a utility's demand to sign the DSA and SA should not be a ground for discontinuance, particularly not without Commission intervention in the process.

As explained further herein, by their Petition, the JU are effectively arguing that UBP Section 2.F.1.a. was intended to allow the JU to assume the role of the Commission in developing and adopting energy market policies, that in so doing the JU can flout the requirements of SAPA, and the JU have unilateral authority to enforce their self-established and self-adopted policy without first seeking Commission intervention to discontinue an ESCO that the *utility* deems to be non-compliant. It strains credulity to assert that the Commission would have adopted UBP Section 2.F.1.a. to have that meaning and intended effect. It is contrary to one of the primary missions of the Commission: to curb utility market power abuses. It is contrary to the Public Service Law that authorizes the Commission to promulgate rules and approve tariffs, not the utilities it regulates. It is contrary to SAPA, which requires potentially affected entities to receive proper notice and an opportunity to comment on proposed compliance obligations and that when those compliance obligations are finalized they be published so that current and potentially affected entities are apprised of the regulatory requirements they must follow. For these reasons, the JU Petition and relief requested should be denied by the Commission.

I. The Business-to-Business Process Did Not Result in a Balanced Agreement

Following a cyber incident in the spring of this year, the JU circulated and sought to require ESCOs doing business on their systems to execute Data Security Agreements (DSAs) and Vendor Risk Assessments (VRAs). In response to requests from the ESCO community, a meeting was held on May 31st with the JU, ESCOs and ESCO representatives, and EDI providers in which the JU reviewed their arguments for imposing the new requirements on ESCOs and in which the ESCOs were able to briefly explain their many significant concerns. Staff attended the meeting as a facilitator.

Following ESCO industry requests for the formal docketing and initiation of an associated regulatory process with respect to the development of DSAs and VRAs, on June 14, 2018, the Commission opened Docket 18-M-0376 to address cyber security protections in the energy marketplace. In so doing, it noted the "business-to-process" that was being utilized by the JU and ESCOs and directed Staff to file a report on its status. The Commission explained that its "goals are to ensure that adequate cyber security protections are in place to protect utility systems and confidential and sensitive customer information, and to explore whether insurance is an efficient and effective vehicle for mitigating any potential financial risks. These issues should be developed to address both the energy services entities, as well as distributed energy resource suppliers." (Order at 3).

Subsequently, the business-to-business process continued, with the JU and ESCO community engaging in another in-person meeting, multiple conference calls and exchanging comments and revised drafts of the DSA and the Self-Attestation (SA) (the successor document to the VRA) documents. The business-to-business process did foster an increased understanding of the JU's

proposed cybersecurity requirements. However, despite many outstanding questions from the ESCO community and remaining areas of substantive disagreement, in an email dated August 16th, the JU stated,

> *The Joint Utilities consider the DSA, and the previously sent Self-Attestation, to be final*. ESEs must submit the completed and signed Self Attestation by August 24, 2018. Modified Self Attestations are not acceptable. As previously stated comments explaining the status of compliance for each question are encouraged so that the Utilities can work with the ESEs to attain adequate security over a reasonable period of time for those ESEs that lack adequate security at this time. If you have already submitted an executed non-modified Self Attestation, you do not need to submit the final Self Attestation. If you submitted a modified or unexecuted Self Attestation, you must submit and execute the final Self Attestation. The final DSA must be executed and submitted to the applicable Utilities by August 31, 2018. (emphasis added).[2]

On September 24, 2018, Staff filed its "Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry." Staff opined that the "business-to-business process has enabled a productive dialogue and has resulted in a balanced DSA."[3] During the business-to-business process, it was also proposed that a cyber security work group be formed to continue the dialogue that had been started and to respond to evolving technological challenges.

In NEM's opinion, Staff's conclusion that a "balanced DSA" was developed during the business-to-business process fails to recognize the utilities' position of superior bargaining power vis a vis the ESCOs. Indeed, ESCOs were faced with a Hobson's choice: either acquiesce to the business-to-business process and sign the agreements or lose the ability to receive information via EDI,

[2] See Joint Utility Message Regarding Data Security Agreement and Self Attestation posted to the Business-to-Business Process webage available at:
http://www3.dps.ny.gov/W/PSCWeb.nsf/All/4A24D0D51395B1F8852582A2004398A3?OpenDocument

[3] Case 18-M-0376, Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry, at page 8.

resulting in the loss of ability to serve their customers and do business. This was one of many reasons the ESCO community sought increased Commission involvement and oversight beyond Staff participation as a "facilitator."

The terms of the agreements being imposed by the JU, that stand as direct competitors in the retail marketplace with ESCOs and control ESCO access to the utility delivery system, are not balanced. The agreements provide the JU with unprecedented and far-reaching control over their ESCO competitors. The JU granted themselves audit rights over ESCO operations, restrict derivative data uses in a manner that could undermine DER product development, restrict locations for ESCO processing and storage of information, and impose a new $5 million cyberinsurance requirement, amongst others.[4]

II. The Commission Has Authority to Promulgate and Adopt Rules, Not the Utilities it Regulates

The JU's heavy-handed conduct prior to and during the business-to-business process is not a reasonable means to develop state policy and should not be legitimized or normalized as a process to be used going forward. The Public Service Law vests the Commission with the authority to promulgate and adopt rules and to approve tariffs, not the utilities that the Commission regulates. Yet, the utilities have sought to assume this Commission function through the business-to-business process. Requiring ESCOs to sign the DSA and SA or face discontinuance is a de facto regulatory mandate by the utilities.

[4] See Case 18-M-0376, Petition for Commission Guidance and Related Request for Modification to the Procedural Schedule of the National Energy Marketers Association, dated August 21, 2018, at pages 7-11.

To be clear, the business-to-business process did not resemble and was not conducted in the same manner as the many stakeholder collaboratives that have been successfully employed to resolve industry issues over the years. Those stakeholder collaboratives were properly noticed, Staff-led, and engaged a diverse cross-section of industry participants in developing resolutions. The results of the stakeholder collaboratives were reported to the Commission, subject to stakeholder comment and then reviewed and acted upon by the Commission. These vital measures were missing from the business-to-business process. Indeed, as the Commission looks to engage new providers of DER services in the New York market, there should be real concern about the chilling effect on investment and participation by competitive entities in markets where utility monopolies abuse their market power and take this type of unilateral action.

III. The Business to Business Process Did Not Satisfy SAPA Requirements

As NEM expressed in prior filings to Docket 18-M-0376 as well as to the business-to-business process, neither the DSA nor the Self Attestation have been filed by the Joint Utilities in the cybersecurity proceeding, in the UBP or UBP DERS proceeding, as a proposed utility tariff, or in any other appropriate venue.[5] The DSA and SA effectively establish cybersecurity policy for the retail energy marketplace in the State of New York and also effectively amend UBP Section 4 and UBP DER Section 2.C, pertaining to the provision of customer information via EDI, by requiring a regime for data access, use, storage and destruction that is far more prescriptive than the Commission has ever considered or required. However, neither of the documents terms and

[5] See Case 18-M-0376, Comments of the National Energy Marketers Association on Cybersecurity Policy, Proposed Data Security Agreement and Self-Attestation Form and Request for Extension of the Self-Attestation Form, dated June 28, 2018; Petition for Commission Guidance and Related Request for Modification to the Procedural Schedule of the National Energy Marketers Association, dated August 21, 2018, both of which submissions are incorporated by reference herein.

conditions have been reviewed and approved by the Commission. Although a DSA was adopted in the context of Community Choice Aggregation, that document differs materially from what the ESCOs are being required to sign and is reflective of a different market construct.[6] Requiring ESCOs to sign the DSA and SA, without first having obtained Commission approval of the documents, is tantamount to the JU establishing regulatory mandates on New York cybersecurity policy for the retail energy marketplace rather than the Commission itself.

The DSA and SA cannot be imposed on the ESCO community without adherence to a SAPA compliant process.[7] No proposed rule incorporating the cybersecurity standards has been propounded and issued for public comment in the New York State Register as required under SAPA § 202(1)(a). The Commission has not reviewed and adopted the DSA and SA as approved policy. No notice of rule adoption has been filed in the New York State Register as required under SAPA §202(5). Such notice is necessary and required under SAPA to establish and apprise entities of their compliance obligations. The DSA and SA also have not been filed by the JU in the online docket files for Case 18-M-0376, 98-M-1343 or 15-M-0180.[8] For example, under these

[6] The terms of the DSA and SA are materially different than those approved by the Commission in Case 14-M-0224 in the DSA for Community Choice Aggregation (CCA). The DSA for CCAs included no provision on customer consent because that market model is premised on opt-out enrollment, wherein no express customer consent for the enrollment is given. The traditional ESCO model requires express customer consent to the transaction. The DSA for CCAs contains no cyberinsurance provision as that requirement was rejected by the Commission. The Commission also rejected the utilities proposal to include provisions on Data Access Controls and a required Information Security Program in the DSA for CCAs because the provisions were "overly prescriptive." The SA that ESCOs are being required to sign by the utilities here includes an extensive regime of data access controls and an information security program that are at least as prescriptive. Importantly, the DSA for CCAs was not proposed or examined in view of its potential extension to the entire ESCO community in Case 14-M-0224 nor were the consequences of doing so.

[7] "[T]he PSC must provide an opportunity to be heard in a meaningful manner and at a meaningful time."[7] National Energy Marketers Association et al. v. New York Public Service Commission, Alb. Co. Index No. 868-16, Decision/Order, dated July 22, 2016.

[8] In Staff's September 24th Report in Case 18-M-0376, Staff stated its intent at page 5 to attach the DSA and SA but those documents are not in the online case file.

circumstances, it is unclear how a potential market entrant would be expected to know that these documents and extensive requirements even exist.

That a business-to-business process was held during which the DSA and SA were discussed does not cure the fatal flaw of SAPA-non-compliance. Nor does the existence of the business-to-business webpage,[9] that is difficult to locate and the existence of which has not been adequately publicized to potentially affected entities. Only *after* the conclusion of the business-to-process with ESCOs were DER providers even engaged in a technical conference to discuss the DSA and SA that is intended to be applied to these entities too. Because the DSA and SA were not developed and approved by the Commission through a SAPA compliant process, the agreements are not valid Commission rules. Therefore, an ESCO's decision not to sign the unapproved agreements does not constitute non-compliance with a Commission rule.

IV. The Utilities Do Not Have the Right to Discontinue ESCO Service Because an ESCO Has Not Signed the DSA or SA

The JU are invoking the language under UBP Section 2.F.1.a. as the purported basis for their "right" to discontinue ESCO service when an ESCO does not execute the DSA and SA. UBP Section 2.F.1.a. provides that a utility may discontinue an ESCO's participation in its retail access program for "[f]ailure to act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice." Section 2.F.2. and 2.F.7. explains the process to be followed to initiate the discontinuance process, including the provision of notice and a cure period.

[9] See http://www3.dps.ny.gov/W/PSCWeb.nsf/All/4A24D0D51395B1F8852582A2004398A3?OpenDocument

In addition, Section 2.F.5. states that the utility "may request permission from the Department to expedite the discontinuance process, upon a showing that it is necessary for safe and adequate service or in the public interest."

To NEM's knowledge, Section 2.F.1.a. has not previously been invoked as the basis for an ESCO discontinuance. When Section 2.F. was originally adopted nearly two decades ago, cybersecurity risks were not in the realm of generally understood or anticipated system security risks. By its terms, Section 2.F.1.a. requires a showing that an ESCO's conduct poses "a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system." However, the type and extent of conduct to satisfy the Section 2.F.1.a. threshold has not heretofore been examined by the Commission. In the absence of such Commission guidance, the JU should not be permitted to exert unchecked discretion in making a determination that an ESCO should be discontinued under this Section.

The JU Petition wrongly and inappropriately construes an ESCO decision *not to sign the agreements* as incontrovertible evidence that the Section 2.F.1.a. standard has been met *without any actual proof* that an individual ESCO's conduct and operations[10] in fact constitute a "significant risk" to the utility distribution system. Throughout the business-to-business process the utilities failed to explicate in quantifiable or verifiable terms the risks to be mitigated and how the requirements embedded in the DSA and SA were reasonably tailored to address those risks.

[10] Cybersecurity policy and any DSA and SA incorporating that policy should be premised on ESCO compliance obligations that are operationally appropriate to the size and scope of an individual ESCO's business and provide flexibility in satisfying compliance requirements. For example, some ESCOs have no interaction with utility EDI systems because they have outsourced the EDI function completely. Those ESCOs pose no threat to the utility system. Another basis of distinction is the extent to which an individual ESCO receives confidential data. For example, ESCOs that do not serve mass market customers, and accordingly would never receive information about a customer's low income status, pose a lower risk.

NEM and its members support the development of reasonable cybersecurity standards for the retail marketplace. However, the utilities did not provide specific, actionable information about the risks posed by ESCO access to data. This is why the DSA and SA utilize an overly broad, blanket approach to the treatment of all ESCOs regardless of individual risk posed, rather than targeted solutions being identified and incorporated in the agreements. Indeed, an ESCO's decision not to sign the DSA or the SA does not mean that the ESCO has not implemented robust cybersecurity measures to protect customer data that are appropriate to the size and scope of its individual business. The ESCO's decision not to sign the DSA or SA could very well be related to the risks and costs associated with signing and implementing agreements that to date have not been subject to Commission scrutiny or received Commission approval.

Moreover, if UBP Section 2.F.1.a. is the provision under which cybersecurity standards are to be imposed on competitive entities, the JU have offered no explanation as to why a corollary provision does not exist in the UBP-DERS. The JU have made clear their intention to extend the application of the DSA and SA to DER providers. However, if a DER provider does not acquiesce to the utility demand to sign the DSA and SA, there is no provision under the UBP-DERS in the form of UBP 2.F.1.a. under which the utility could seek to discontinue service. Nor does the UBP for ESCOs apply to DER suppliers.

UBP Section 2.F.1.a. was not intended to give the utilities unfettered discretion to demand prescriptive unvetted contracts to be signed by ESCOs participating in retail access programs allegedly in the name of system reliability. The JU's Petition asserting such a "right" under this Section should be rejected.

V. The Utilities Petition to Discontinue ESCO Service Without Commission Intervention Should Be Denied

The JU's Petition is not only seeking Commission approval of the ability to discontinue an ESCO's participation in a retail access program for the ESCO's decision not to execute the DSA and SA but also to affirm the JU's ability "to initiate the discontinuance process pursuant to UBP Section 2(F)(2) *without intervention of the Commission."* This should also be rejected by the Commission. While Section 2.F.7.a. allows the utility to "discontinue participation as soon as practicable" for ESCO conduct posing "a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system," UBP Section 2.F.5. clearly requires the utility to "request permission from the Department to expedite the discontinuance process, upon a showing that it is necessary for safe and adequate service or in the public interest." Read together these provisions reflect a clear understanding that Commission intervention in the process as an objective arbiter is a necessary and required check on the utilities' ability to discontinue ESCO service. Staff's Report in Case 18-M-0376 supports this – "The UBP details the discontinuance process, including timeframes, and includes participation by Staff."[11]

The JU are effectively requesting in the Petition that the Commission cede its oversight role, as expressed in UBP Section 2,[12] to the utilities by permitting the JU to discontinue an ESCO without

[11] Case 18-M-0376, Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber security in the Retail Access Industry, dated September 24, 2018, at 2.

[12] UBP Section 2.D.5. sets forth categories of non-compliance for which the Commission may impose consequences on ESCOs, including suspension of the ability to participate in retail access programs and suspension of ESCO eligibility to operate in New York. Subsection 2.D.5.k. includes "any of the reasons stated in Subdivision F of this Section" as a category. UBP Section 2.D.6.a. delineates the process that will be followed when the Commission is determining consequences for ESCO non-compliance, including notice to the ESCO and an opportunity to be heard. However, as explained in the previous sections of this response, the DSA and SA have not been subject to Commission review or received Commission approval and have not been published as proposed or final Commission requirements as is necessary and required under SAPA to establish and apprise entities of their compliance obligations. Therefore, if an ESCO does not acquiesce to the utilities demand to execute the DSA and SA this should not be actionable as ESCO "non-compliance" under UBP Section 2.D.5. and 2.D.6.

Commission intervention. NEM submits that Commission intervention is particularly vital here, where the Commission has not previously adopted cybersecurity policy for the retail marketplace, where precedent interpreting and applying UBP Section 2.F.1.a. has not been established, where the utility's potential to abuse its market power is significant and where the consequences to the ESCO of discontinuance are severe and irreparable. Moreover, UBP Section 2.F.1.a. requires a case-specific inquiry into whether individual ESCO conduct is causing "a significant risk" to the distribution utility system.

It would be an extreme and dangerous precedent to interpret Section 2.F.1.a. in the manner requested by the JU – to allow the utility to be the sole arbiter of a dispute to which it is also one of the parties and concerning agreements that it authored. Interpreting Section 2.F.1.a. to allow the JU to discontinue an ESCO that has not executed the agreements, agreements that are not Commission-approved and have not been filed in any Commission docket, and without Commission intervention, would compound the harmful precedent.

In addition, UBP Section 8 sets forth a dispute resolution process available at the Department to resolve disputes between utilities and ESCOs. UBP Section 8 delineates a process to be followed under which written notice is provided to the opposing party and Staff, a procedure for the parties to attempt to achieve a mutually acceptable resolution, and if a mutually acceptable resolution is not reached within forty calendar days, the ability to request an initial decision from the Department and appeal such decision to the Commission. UBP Section 8.B.2. also sets forth an expedited process to address emergency situations, including for example, "a threat to public safety or system reliability or a significant financial risk to the parties or the public." The process to be followed for expedited resolution is initiated by the filing of a formal dispute resolution request with the Secretary and a copy to other involved parties and Staff. The type and extent of process

afforded under UBP Section 8 is needed to afford an ESCO with the opportunity for an objective assessment of the decision not to sign the JU's DSA and SA.

VI. Conclusion

For the foregoing reasons, NEM respectfully recommends that the JU's Petition for a Declaratory Ruling regarding their "right" to discontinue ESCO service if an ESCO has not executed a DSA and SA, and to do so without Commission intervention, should be rejected.

Respectfully submitted,

s/Craig G. Goodman

Craig G. Goodman, Esq.
President
Stacey Rantala
Director, Regulatory Services
National Energy Marketers Association
3333 K Street, NW, Suite 110
Washington, D.C. 20007
Tel: (202) 333-3288
Email: cgoodman@energymarketers.com;
srantala@energymarketers.com

Dated: November 30, 2018.