**STATE OF NEW YORK**
**PUBLIC SERVICE COMMISSION**

| | | |
|---|---|---|
| **Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place** | **)** **)** **)** | **Case 18-M-0376** |
| **In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products** | **)** **)** **)** | **Case 15-M-0180** |

**Response of the**
**National Energy Marketers Association**
**To the Joint Utilities Petition Regarding Data Security Agreement**

The National Energy Marketers Association (NEM)[1] hereby respectfully submits this Response to 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," [hereinafter "February Petition"] dated February 4, 2019. The Commission issued a Notice Soliciting Comments on the February Petition and other related Petitions on February 20, 2019, and a Notice of Proposed Rulemaking on the establishment of cyber security requirements, including the February Petition, was published in the State Register on February 27, 2019.

[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.

In the February Petition the Joint Utilities (JU) are requesting that the Commission:

1) Confirm that the business-to-business process that was used to develop the Data Security Agreement (DSA) and the Self-Attestation (SA) form was appropriate;
2) Authorize the amendment of the DSA going forward through the business-to-business process;
3) Approve minimum standard requirements in the DSA subject to continuing possible modification as necessary to accommodate technological changes; and
4) Affirm JU authority to require Energy Services Entities (ESEs) to submit and execute a DSA; and to disconnect an ESE from the utility's IT system for failure to do so. (February Petition at 1-2).

The February Petition follows an earlier filing made by the JU in Dockets 98-M-1343 and 18-M-0376. The November 9, 2018, filing was entitled "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" [hereinafter "November Petition"]. In the November Petition the JU requested that the Commission "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." (November Petition at 1-2). In the November Petition, the JU not only claimed the right to discontinue ESCO service, they also asserted that "the UBPs permit individual utilities to initiate the discontinuance process pursuant to UBP Section 2(F)(2) *without intervention of the Commission*." (emphasis added) (November Petition at 8). The February Petition notes the filing of the November Petition

and states "[t]his Petition seeks similar treatment of for [sic] ESEs, Direct Customers and other current and future entities as it relates to customer information. The Joint Utilities expect that the ESCO Declaratory Ruling Petition will be subsumed into this request. Operations system interconnections between the utilities and DERS are not included or discussed under this Petition and will require different and more stringent security standards." (February Petition at note 3).

NEM supports the development and implementation of reasonable cybersecurity standards for the retail energy marketplace. However, as explained in this and prior filings,[2] the Data Security Agreement (DSA) and Self Attestation (SA) are the result of a fundamentally flawed process, one that cannot be remedied by the after-the-fact fixes the utilities attempt to utilize in the February Petition. The Commission is entrusted with the authority to develop, implement and enforce energy policies in the State of New York. The JU have usurped the Commission's policymaking authority in the business-to-business process to develop, implement and enforce cybersecurity policy for the retail energy marketplace in the State of New York that heretofore did not exist. The JU, direct competitors with ESCOs and ESEs, are exercising utility monopoly market power to unreasonably restrict ESCOs and other ESEs from accessing their systems and thereby cause these entities to be unable to serve customers. For these reasons, the Commission should affirm that reliance on a SAPA-compliant process is necessary and will be relied upon for the establishment of reasonable cybersecurity policy for the retail energy marketplace in New York.

[2] 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; 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; Cases 98-M-1343 and 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, dated November 30, 2018, all of which submissions are incorporated by reference herein.

1) **The Proper Manner to Develop and Implement New York State Cybersecurity Policy is Through the Rulemaking Process at the Commission, Not a Utility-Controlled Business-to-Business Process**

Contrary to the assertions of the JU, the business-to-business process that was used to develop the DSA and SA form was not appropriate. The business-to-business process that developed the DSA and SA establishes compliance requirements for ESCOs and other ESEs that effectively adopts cybersecurity policy for the retail energy marketplace in New York where none has existed before. The DSA and SA also effectively amend UBP Section 4 and UBP Section 2.C. pertaining to the provision of customer information via EDI by requiring a regime for data access, use, storage and destruction far more prescriptive than the Commission has ever considered or required. The appropriate manner to establish retail energy market policy is for the Commission to issue a notice of proposed rulemaking, gather stakeholder feedback and for the Commission to then adopt policy premised on the record developed. The Commission, as an objective arbiter, weighs the parties' respective positions and adopts policy that reasonably balances the objectives to be achieved and the means used to achieve them. The Public Service Law vests the Commission with the authority to promulgate and adopt rules and to approve tariffs. That function is the exclusive province of the Commission and does not lie with the utilities it regulates nor can it be delegated to them. Only *after* the Commission has adopted reasonable cybersecurity policy should a business-to-business process be utilized to work on the technical implementation details.

The business-to-business process utilized in the instant case and the relief now being requested by the JU in their February Petition and November Petition spins the SAPA rulemaking requirements on their head, anointing the JU as retail energy market policymakers and enforcers. The JU's heavy-handed conduct 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.[3] It is not appropriate for utilities to exercise their market power to restrict access to their systems to ESCOs and other ESEs through the conduct of a business-to-business process the results of which ESCOs and other ESESs had little influence over and for whom non-acquiescence results in the loss of the ability to do business and serve consumers.[4]

The JU maintain that a "robust and substantial process supported the development of the DSA." (February Petition at 14). NEM explained in its response to the November Petition that the

[3] Indicative of this heavy-handed approach, the ESCOs engaged in good faith with the JU in in-person meetings, multiple conference calls and exchanging comments and revised drafts of the DSA and the SA, but many outstanding questions from the ESCO community and remaining areas of substantive disagreement persisted. However, 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). 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

[4] Staff's participation as a "facilitator" of the business-to-business process may not be sufficient to constitute "active supervision" by the Commission necessary for state action immunity. The U.S. Supreme Court recognized that conduct of private parties (such as utilities) could be afforded with State immunity to antitrust laws. Parker v. Brown, 317 U.S. 341 (1943). However, a State's immunity does not extend to anti-competitive conduct by a private party "unless, first, the State has articulated a clear and affirmative policy to allow the anticompetitive conduct, and second, the State provides active supervision of anticompetitive conduct undertaken by [the] private actor[ ]." FTC v. Ticor Title Ins. Co., 504 U.S. 621, 631 (1992). The Supreme Court also found that even a regulated utility must "comply with antitrust standards to the extent that it engaged in business activity in competitive areas of the economy." Cantor v. Detroit Edison Co., 428 U.S. 579, 596 (1976).

Moreover, this Commission found that, "[u[tilities that act in the competitive arena and in a manner that would otherwise run afoul of the antitrust laws should not escape accountability for their actions on the basis of the state action exemption from those laws." Accordingly, the NYPSC held "that any utility activities that impede the development of the competitive market, or the development of competition in potentially competitive markets (and are not otherwise actively supervised), would not be consistent with our policies and, therefore, are not eligible for the exemption." New York Public Service Commission, Case 00-M-0504, Statement of Policy on Further Steps Toward Competition in Retail Energy Markets, issued August 25, 2004, at page 43.

business-to-business process did not satisfy the procedural requirements of SAPA.[5] As of the time of filing of NEM's comments on the November Petition neither the DSA nor the SA had 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 thereby preventing potentially affected entities from receiving notice that the cyber security policy was being developed. SAPA requires the publication of notice of the proposed rule under SAPA Section 202(1)(a), Commission deliberation after receipt of stakeholder comment, and the issuance of a notice of adoption of a Commission rule under SAPA Section 202(5). None of those steps were taken prior to the JU seeking to enforce (unjustifiedly and without authority) the DSA and SA against ESCOs. Contrary to the JU arguments, the DSA that was adopted in the context of Community Choice Aggregation[6] differs materially from the DSA and SA that the ESCOs and other ESEs are being required to sign and is reflective of a different market construct and cannot be used as a justification for skirting SAPA requirements.

In the February Petition the JU seek to cure the process deficiencies identified by NEM in its Response to the November Petition. The operative fact here is that the process deficiencies *have*

[5] Cases 98-M-1343 and 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, dated November 30, 2018, pages 6-8.

[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.

*already taken place*.[7] Potentially-affected entities were not apprised of the business-to-business process before or during the time it was taking place – the time when the terms of the DSA and SA were being developed and when participation is vital to affecting the ultimate outcome. That the JU finally filed a copy of DSA and SA in Dockets 18-M-0376 and 15-M-0180 in February 2019 is not sufficient to undo the harm to the potentially affected entities (curiously the JU still did not file the DSA and SA in Docket 98-M-1343 notwithstanding the direct connection to the provisions of the UBP). Shining light on these policies and requirements after-the-fact of their development is not sufficient to ensure an informed dialogue or to afford parties with a *real* opportunity to inform or influence the results. Due process requires a meaningful opportunity for participation. Meeting notices and documents must be published to official Commission dockets on the Commission website. In the case of the ESCO business-to-business process, no notice of the initial meeting held on May 31, 2018, was published on the Commission website in a Commission docket. Indeed, the first business-to-business process meeting occurred before Docket 18-M-0376 was even opened by the Commission on June 14, 2018.[8] Compounding the problem, the JU communicated to the business-to-business process participants through a subpage of the EDI workgroup page[9] that was not well-publicized or generally known.

The consequences of the JU strategy to conduct the business-to-business process in this manner have been evident in the protests of the Distributed Energy Resource (DER) community as well, that rightfully object to being subjected to the terms of the DSA and SA for which their input was not sought until after the conclusion of the business-to-business process with the ESCO

[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] Case 18-M-0376, Order Instituting Proceeding, issued June 14, 2018.
[9] See http://www3.dps.ny.gov/W/PSCWeb.nsf/All/4A24D0D51395B1F8852582A2004398A3?OpenDocument

community. Now the JU would like to believe that the proverbial "die has been cast" in the matter. However, if the intention was to develop a one-size-fits-all approach in the DSA and SA, the DER suppliers should have been engaged in the business-to-business process alongside the ESCOs.

The JU also now appear to be alternatively arguing that a SAPA compliant rulemaking process was unnecessary because, "ESEs should be treated as any other vendor, i.e., ESEs should be required to meet the Joint Utilities terms and conditions, which would include cyber security terms, as the Joint Utilities have the right to set and negotiate transactional terms and conditions independently." (February Petition at 3). The argument that an ESCO is a vendor of the utility should be squarely rejected. A vendor of the utility has the option to exit contract negotiations with a utility and to serve a different client if the vendor does not agree with the terms the utility is requiring. Not so with an ESCO. ESCOs are completely reliant upon access to the utility delivery infrastructure and IT system in order to serve their customers. The utility monopoly has superior bargaining power over the ESCOs with the looming threat of disconnection if ESCOs do not acquiesce to the utility's demands for access to its systems. Given this dynamic, it is imperative that the Commission rein in the utilities' attempted market power abuse in the instant case and insist upon a SAPA compliant rulemaking process for the development of state cybersecurity policy.

**2) After the Commission Adopts Cybersecurity Policy for the Retail Energy Marketplace, a Business-to-Business Process May Be Utilized to Address Technical Implementation Details and Identify Proposed Modifications to the Commission**

The Commission should not legitimize or endorse a business-to-business process as a means for adopting and establishing energy market policy. A business-to-business process is appropriate only *after* the Commission has adopted a cybersecurity policy for the retail energy marketplace.

The business-to-business process should be narrowly focused on addressing technical implementation details, not making policy determinations that favor one stakeholder over another. A business-to-business process may also be useful in identifying technological changes requiring modifications to the DSA and SA and suggesting proposed modifications to the Commission. Proposed modifications to the DSA or SA may not be the product of group consensus, and multiple appropriate modifications may be suggested by different stakeholders. After the proposed modifications are submitted to the Commission, it should be followed with a SAPA-compliant process, including notice and the opportunity for stakeholder comment, prior to Commission adoption.

### 3) The Commission Should Adopt Reasonable Cybersecurity Standards for the Retail Energy Marketplace

The JU are requesting in the February Petition that the Commission approve minimum standard requirements in the DSA subject to continuing possible modification as may be necessary to accommodate technological changes. The JU suggest that minimum standard requirements in the DSA should include:

> "(1) specify compliance with the Uniform Business Practices ("UBP"), UBP DERS, or other applicable Commission rules; (2) address the transfer of information; (3) maintain the confidentiality of Joint Utilities and the ESCOs, DERS, Direct Customers, and their applicable contractors (collectively, "Energy Service Entities" or "ESEs") information, including the protection of customer data; (4) requiring the return and destruction of information; (5) address each Party's responsibility and liability for data security incidents; (6) require cyber security insurance; (7) define minimum cyber security requirements; (8) address how to determine whether ESEs have and maintain minimum levels of cyber security; and (9) require ESE indemnification of the Joint Utilities." (February Petition at 1-2).

NEM has suggested and sought Commission guidance in the establishment of reasonable statewide cybersecurity policy for the retail energy marketplace since the business-to-business process was

initiated. Commission establishment and approval of standard terms and conditions would be helpful in this regard. However, the DSA and SA that resulted from business-to-business process are not balanced documents, and the requirements embedded in them should be viewed in that lens. The DSA and SA favor the entities that propounded the documents, namely the JU. The Commission should evaluate the terms and conditions as such, with particular regard for how the data use, storage, and access restrictions will impede availability of innovative energy products and services and thereby thwart the realization of REV goals.

As explained in prior filings to the Commission, there are many provisions and terms in the DSA and SA that have the effect of setting cybersecurity policy and precedent and also have the effect of amending the UBP and UBP DER. These provisions must be properly vetted through a SAPA compliant process and approved by the Commission, before creating an ESCO compliance obligation. These provisions include:

- **Customer Data** - The most important term used in the documents is "Confidential Utility Information" (CUI). The DSA and SA set forth its approved uses, how it can be transported, stored, and destroyed, and the consequences for a data breach. The DSA also includes a definition of "Confidential ESE [Energy Service Entity] Information" as well as "Confidential Information," which refers to both CUI and CEI, collectively.

  The nexus between REV and these documents is readily-apparent. REV is premised on customer engagement and market participation enabled by access to customer data.[10] While the Joint Utilities have advocated for a focus on "confidential utility information,"

[10] "REV will establish markets so that customers and third parties can be active participants, to achieve dynamic load management on a system-wide scale, resulting in a more efficient and secure electric system including better utilization of bulk generation and transmission resources." Case 14-M-0101, Order Adopting Regulatory Policy Framework and Implementation Plan, issued February 26, 2015, page11.

the modern REV era requires that this data be viewed and denominated as what it is – customer data. It is customer data for which the customer has the right to direct that it be accessed, used, and analyzed by ESCOs and other authorized parties so that they can design and develop innovative products and services to serve the customer.[11] The Joint Utilities have market power in data.[12] The DSA and SA should be constructed so as to mitigate that market power and to empower consumer choices.

For instance, DSA Section 14.a. prohibits ESCOs from creating or maintaining data that is derivative of CUI, subject to certain exclusions. The exclusions enumerated may be too narrow to accommodate or anticipate derivative data uses that will fuel DER product and service development. This clearly runs counter to REV goals - "Ready access to information regarding customer energy usage is vital to the success of DER markets. For DER developers, information about a potential customer's energy usage is necessary to design products tailored to the consumer's needs."[13] In other words, ESCOs analyze customer information to derive data that drives customer-focused product innovation. To be clear, UBP Section 4.F. already clearly sets forth ESCO obligations with respect to customer data as well as prohibited uses and practices.[14] The DSA exceeds these requirements of the UBP.

---

[11] "Technology innovators and third party aggregators (energy service companies, retail suppliers and demand-management companies) will develop products and services that enable full customer engagement." Id. at 12.

[12] In its filing on proposed fees for Community Choice Aggregation data, ConEd explained that "only a utility has access to all customers' retail choice status, block status, energy usage data, and customer information." Case 14-M-0224, Petition to Establish Platform Service Revenues, dated August 5, 2016, page 7.

[13] Case 14-M-0101, Order Adopting a Ratemaking and Utility Revenue Model Policy Framework, issued May 19, 2016, page 137.

[14] UBP Section 4.F. provides that,

> An ESCO, its employees, agents, and designees, are prohibited from selling, disclosing or providing any customer information obtained from a distribution utility or MDSP, in accordance with this Section, to others, including their affiliates, unless such sale, disclosure or provision is required to facilitate or maintain service to the customer or is specifically authorized by the customer or required by legal

- **<u>Cyber Insurance</u>** – In opening this cybersecurity proceeding, one of the issues identified for exploration by the Commission was "whether insurance is an efficient and effective vehicle for mitigating any potential financial risks."[15] The Joint Utilities have steadfastly maintained that a cyber insurance requirement should be applied to ESCOs, although they reduced the amount of the DSA cyber insurance requirement to $5 million rather than the $10 million that was originally proposed and also agreed to remove the proposal that utilities be included as a named insured. The propriety of this requirement should be subject to Commission scrutiny before such a policy is adopted and ESCOs are subject to the imposition of such a significant compliance cost.

  If a cybersecurity insurance requirement is imposed, it should be commensurate with the nature of the data to be protected, the extent of ESCO interaction with utility systems (some ESCOs completely outsource the EDI function and do not interact with the utility EDI system), the risk posed by those interactions, and the cybersecurity measures the ESCO has implemented to prevent a data breach. In addition, if a cybersecurity insurance requirement is imposed, ESCOs should have flexibility in satisfying the requirement, for example, by allowing the ESCO to be self-insured, and allowing use of letters of credit or other similar security instruments.

  Throughout the business-to-business process NEM and other stakeholders questioned the basis for the imposition of the cyber insurance requirement and requested that the risks underlying the requirement be identified and quantified. The JU offered general anecdotes

authority. If such authorization is requested from the customer, the ESCO shall, prior to authorization, describe to the customer the information it intends to release and the recipient of the information.

[15] Case 18-M-0376, Order Instituting Proceeding, issued June 14, 2018, page 3.

for a cyber insurance requirement, rather than provide a rational basis, throughout the duration of the ESCO business-to-business process. In the February Petition the JU finally produced a study about the costs of cyber security incidents. (February Petition at page 6 and Attachments 7 and 8). The study cites the cost of cyber incidents for financial service, utility and energy companies. Critically, the study does not appear to distinguish the costs and risks faced by a regulated utility charged with maintaining delivery infrastructure and IT systems versus the costs and risks for ESEs whose interaction with utility IT systems vary significantly (with some ESEs outsourcing EDI functions completely). ESCOs do not own or operate utility-scale assets. As such, the costs of a cyber incident in the study would be significantly overstated and not reflective of risks posed by ESEs.[16] This is a critical distinction that we have been making since the inception of the business-to-business process.

ESCOs and other ESEs have explained that the cost of cyber insurance will force innovators out of the marketplace, prevent market entry resulting in the delay in realization of REV goals (or perhaps never), which will result in the imposition of costs on consumers. NEM submits that an alternative consideration to the imposition of onerous, unjustified cyber insurance costs on the marketplace is for the utilities to become certified by the Department of Homeland Security under the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act.[17] The SAFETY Act[18] was passed in 2002 in response to the September 11th attacks as a means to encourage companies to develop anti-

[16] February Petition, Attachment 8, p. 44, 54-55.
[17] 6 U.S.C. §§ 441-444. See also www.safetyact.gov.
[18] For an explanation of the SAFETY Act provisions, liability and risk management benefits, and certification process see SAFETY Act Decreases Private Sector Risk and Liability, Today's General Counsel, Winter 2019, p. 58-61; Beyond CIP Compliance: Managing Cyber and Physical Security Risk, T&D World, November 16, 2015.

terrorism technologies by providing safeguards, including liability protections.[19] Both Southern Company[20] and PSE&G[21] have recently been certified under the SAFETY Act.

Of significance to the instant case, the SAFETY Act includes "information technology"[22] as a category of eligible anti-terrorism technology, and SAFETY Act regulations recognize "cyber terrorism"[23] as falling within the Act's definition of "act of terrorism."[24] A company's internal program for securing its own assets may seek protection under the Act. As such, the SAFETY Act can be an important component of cybersecurity risk management in the utility industry that is safeguarding its delivery infrastructure and IT systems from cyber attacks. Moreover, the liability protections extend not just to the SAFETY-certified entity itself, but also to downstream users involved in the "use or operation of qualified anti-terrorism technologies"[25] – in other words utility certification

[19] 6 U.S.C. 443(a)-(c).

[20] Southern Company received SAFETY Act certification on September 19, 2018, for the following:
"The Southern Company and its named subsidiaries provide the Cybersecurity Risk Management Program (the "Technology"). The Technology is an enterprise-wide cyber risk mitigation program that advances Company cybersecurity goals in electricity generation, transmission, and distribution, gas services, business corporate services, and other activities. Administered at the board, executive, and management levels, the Technology manages cybersecurity risk through governance, strategic direction, network security and data protection, business assurance, incident response, training, and policies and guidance. This Designation and Certification will expire on October 31, 2023."

[21] PSE&G received SAFETY Act certification on July 09, 2018, for the following:
"Public Service Enterprise Group Incorporated ("PSEG"), through its subsidiary, Public Service Electric and Gas Company ("PSE&G"), provides PSEG Holistic Security Model (the "Technology"). The Technology is a customized program designed to identify and reduce risks based on comprehensive planning processes and protocols and physical security measures protecting PSE&G critical energy infrastructure and assets at five critical sites within the New Jersey PSE&G Service Area. The Technology consists of the following core components: infrastructure risk-rating tool and vulnerability assessment processes; business interruption management model; industry liaison security model; threat level advisory system; enterprise security plans and plans; security awareness training program; background checks and insider threat mitigation; security command centers; physical security measures and equipment; procurement processes for physical security services and equipment; and physical security exercises and assessments. This Designation will expire on July 31, 2023."

[22] 6 U.S.C. 444(1).

[23] Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), Federal Register Vol. 71, No. 110, June 8, 2006, p. 33154.

[24] 6 U.S.C. 444(2).

[25] 6 U.S.C. 443(a)(3). The preamble to the SAFETY Act regulations explains that, "Such cause of action may be brought only against the Seller of the QATT and may not be brought against the buyers, buyers' contractors,

would limit utility liability and limit liability of ESCOs and other ESEs that interact with the utility's system as well. This limitation of liability and risk under the SAFETY Act should commensurately affect cyber insurance coverage. Managing costs and risks in this fashion would benefit all consumers.

- **Third-Party Representatives** – The DSA applies a number of significant compliance obligations on "Third Party Representatives" used by an ESCO, including direct liability to the utility for a data breach, submission to utility audits, compliance with utility security assessments, data processing and storage requirements, and to abide by the applicable UBP or UBP DER.[26] The term "Third-Party Representative" is defined in the DSA to refer to ESCO contractors and subcontractors "that store, transmit or process" CUI. The definition is too broad, encompasses entities that do not pose a real risk to the utility system and imposes unreasonable compliance obligations on these entities where a Non-Disclosure Agreement between the ESCO and Third-Party Representative would be sufficient to ensure customer data security.

- **Restrictions on Locations for Processing and Storage of Information** – The DSA and SA restrict ESCO processing and storage of "confidential utility information" to locations in the U.S. and Canada, unless the utility otherwise agrees in writing. This is an overly restrictive intrusion into ESCO business operations by the JU. The JU maintain that this

downstream users of the Qualified Anti-Terrorism Technology, the Seller's suppliers or contractors, or any other person or entity. . ." Preamble to Final Rule, 6 CFR Part 25, at 33150.

[26] In its review of the role of energy brokers and other third parties in the marketplace, the Commission plainly stated that "[s]ince they are not ESCOs, these third parties are not themselves subject to the UBP, and are subject only to regulation under the State's general consumer protection statutes." Cases 12-M-0476, et.al., Order Taking Actions to Improve the Residential and Small Non-Residential Retail Access Markets, issued February 25, 2014, page 39.

restriction is justified by federal Export Control laws. That interpretation is subject to dispute by ESCOs[27] and should be reviewed by the Commission.

- **Utility Audit Rights of ESCO Operations** – The DSA includes a requirement to allow utilities to audit ESCO operations. The DSA permits alternatives to a utility audit, such as a SOC II Type 2 report or a third-party auditor. However, concerns about permitting the utility, a business partner and direct competitor, to access ESCO confidential and proprietary systems remain. The exact process to be utilized in the audit also remains unclear. Also, PCI DSS[28] compliance by an ESCO should be considered as an alternative to the utility audit.

- **Return and Destruction of Information** – The DSA requires ESCOs to return and destroy "confidential utility information" within thirty days of utility demand, although recognizing an exception for information "required to be maintained by governmental administrative rule or law or necessary for legitimate business or legal needs."

- **Data Security Incident** – The DSA includes a process to be followed in the case of a data security incident involving "confidential utility information" processed by or on an ESCO's behalf. New York law already prescribes a process to be followed in the case of the "breach of the security of the system."[29] The DSA requirements provide the utility with too much discretion, in a situation that is already addressed under New York law. The

[27] See, e.g., Proposed List of Pre-Approved Countries for Data Transfers, submitted by New York Retail Choice Coalition and Supporting ESCOs in Case 18-M-0376, dated August 2, 2018.
[28] The Payment Card Industry Data Security Standard (PCI DSS) refers to payment security standards that ensure all sellers safely and securely accept, store, process, and transmit cardholder data during a credit card transaction. See https://www.pcisecuritystandards.org See also Case 13-M-0178, Order Directing the Creation of an Implementation Plan, issued August 19, 2013, page 8, n. 1 (Commission citing favorably to the PCI Security Standards in reference to the utilities cybersecurity programs). Many ESCOs are already PCI DSS compliant.
[29] NY GBL § 899-aa.

DSA requires an ESCO to provide written notice to the utility within forty-eight hours of a data security incident. The utility should also have a mutual obligation to notify ESCOs of a data security incident so that ESCOs can protect their customers.

- **Self-Attestation Form Requirements** - The SA requires each ESCO to implement an "Information Security Policy," numerous IT safeguards, data storage requirements, and employee screening and training requirements. This is an extensive data security regime, and every element will become cybersecurity policy of the State.

  The DSA states that the "Utility *will* comply with the security requirements set forth in its Assessment." (emphasis added). The utilities have maintained throughout the discussions that their cybersecurity measures are confidential. What is known is that, for example, the SA requires ESCO adoption of industry best practices for the encryption of "confidential utility information" when in transit. Industry best practice utilized in other retail choice jurisdictions is NAESB EDM Version 1.6, but at the time of the ESCO business-to-business process the standard in New York was only GISB EDM Version 1.4.[30] The upgrade to NAESB EDM Version 1.6 was only initiated in the EDI workgroup after the ESCO business-to-business process had concluded.[31]

[30] Case 98-M-0667, Technical Operating Profile for Electronic Data Interchange in New York, Ver 1.5, April 30, 2018, note 9.
[31] Case 98-M-0667, November 2018 Report on EDI Standards Development, dated November 30, 2018.

**4) The Commission Should Reject the JU's Suggestion of Unfettered Authority to Develop and Implement State Cybersecurity Policy and to Enforce the Illegitimately Developed Policy Against Competitors**

The JU's request for Commission "affirmation" of their authority to require ESEs to submit and execute a DSA and to disconnect an ESE from the utility's IT system for failure to do so should be rejected. As explained in the previous sections of these comments, the heavy-handed business-to-business process conducted by the JU with the ESCOs to develop the DSA and SA was not a legitimate means for developing and implementing state cybersecurity policy for the State. The bad precedent of relying on an illegitimate process to set State policy should not be compounded by finding a right in the JU to disconnect ESCOs for failure to execute the documents resulting from the flawed process.

The JU assert that UBP Section 2.F.1.a. provides them with a basis for disconnecting ESCOs for failure to execute the DSA. 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. 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." The JU would interpret that provision such that an ESCO's decision not to execute the DSA would constitute incontrovertible evidence of a "significant risk" to the utility system without any inquiry into whether the ESCO's

operations or conduct[32] in fact posed such a risk. The ESCO's decision not to sign the DSA may have much more to do with the risks and costs of executing a document that would establish significant compliance obligations but has not been reviewed or approved by the Commission.

The JU also falsely equate ESCOs and other ESEs to vendors in this regard, maintaining that they "do not contract with vendors that do not meet their required cyber security terms," and "ESEs have not demonstrated any reason that they should receive different treatment." (February Petition at 13). The comparison of ESCOs and other ESEs to utility vendors doesn't hold water. The JU control ESCOs and other ESEs access to the delivery infrastructure and IT systems so that these entities can provide service to their customers. A vendor is rendering a service or product to the utility and has the option to reject a utility's terms and conditions and work with a different client. Not so for the ESCO or other ESE, that has no choice but to acquiesce to the utility's terms and conditions in order to serve its customers or go out of business.

To NEM's knowledge, 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. Moreover, it should be construed in such a way that it can only be invoked with respect to "significant risks," as opposed to disputes between the utility and an ESCO. UBP Section 2.F.1.a. was not intended to give the utilities unfettered

[32] 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.

discretion to demand prescriptive unvetted contracts to be signed by ESCOs participating in retail access programs allegedly in the name of system reliability.

NEM also notes, because the February Petition applies to ESEs and not just ESCOs, that UBP Section 2.F.1.a. has no corollary provision in the UBP-DERS. In other words, 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.

The JU's November Petition sought 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 and also the affirmation of the JU's ability "to initiate the discontinuance process pursuant to UBP Section 2(F)(2) *without intervention of the Commission."*[33] The JU's February Petition does not make use of same verbiage regarding discontinuance "without intervention of the Commission." However, that may be subsumed within the February Petition as it incorporates the November Petition.[34] As stated in NEM's Response to the November Petition, the JU's suggestion should be squarely 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

[33] Utility disconnection of an ESCO without Commission intervention would also implicate the concerns identified in supra note 4.
[34] February Petition at note 3.

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 proposition – "The UBP details the discontinuance process, including timeframes, and includes participation by Staff."[35]

The JU were effectively requesting in the November Petition that the Commission cede its oversight role, as expressed in UBP Section 2,[36] to the utilities by permitting the JU to discontinue an ESCO without 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

[35] 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.

[36] 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 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-approved and without Commission intervention, would compound the harmful precedent.

NEM additionally notes that UBP Section 8 sets forth a dispute resolution process available at the Department for utilities and ESCOs. UBP Section 8 sets forth 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.

**Conclusion**

For the foregoing reasons, NEM respectfully recommends that the Commission affirm that reliance on a SAPA-compliant rulemaking process is necessary and will be relied upon for the establishment of reasonable cybersecurity policy for the retail energy marketplace in New York.

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: April 26, 2019.