STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission	**)**	
Regarding Cyber Security Protocols and	**)**	**Case 18-M-0376**
Protections in the Energy Market Place	**)**	

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

The National Energy Marketers Association (NEM)[1] and its members recognize the importance of data security to consumers and are committed to protecting that data. NEM believes that each customer in the retail marketplace owns its own data and can direct which entity is authorized to access and use that data. NEM supports the development of industrywide cybersecurity practices and processes pertaining to the safe and secure transmission, processing, storage and disposal of customer data that mitigate the potential occurrence of data breaches in the first instance. It is also important to differentiate between that which constitutes good cybersecurity business practice versus that which is overly proscriptive and overly burdensome. The need for utilities to secure their systems as network grid operators is significantly heightened as compared with ESCOs. Utility-scale cybersecurity requirements should not be imposed on ESCOs.

The majority of the New York utilities have recently required that ESCOs sign Data Security Agreements (DSAs) and Self-Attestation of Information Security Controls [hereinafter "Self-Attestation forms"]. The utilities maintain that the DSAs and Self-Attestation forms are now needed and will be required for ESCOs receiving customer information from the utilities via EDI transactions. The Commission subsequently opened a proceeding on Cyber Security Protocols and Protections in the Energy Market Place with the goals of "ensur[ing] 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."[2] The Secretary issued a letter on June 22, 2018, accepting comments in this Commission docket. NEM respectfully files these comments with the Commission to aid in the creation of a record to support those goals.

NEM has a number of concerns about the DSA and Self-Attestation form and appreciates the opportunity to share its comments. NEM also respectfully requests that the deadline for executing the Self-Attestation form be extended and aligned to correspond with the process for consideration of the DSA as explained in Section II of these comments.

---

[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. This document reflects the views of NEM and does not necessarily reflect the views of any specific member of the Association. These comments are not intended to serve as a waiver of any rights, arguments, claims or remedies, all of which NEM expressly reserves.

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

The Commission did approve a DSA for the specific market construct of Community Choice Aggregation (CCA) programs.[3] While not controlling, it is nonetheless noteworthy that the DSA that was approved for the CCA programs varies from what the utilities are requiring the ESCOs to sign now.[4] An important distinction between the CCA market construct and the historical retail choice model that has been employed in New York is that the municipalities and ESCOs in the CCAs receive customer information without the customers' express authorization because customers participate in CCAs on an opt-out basis. Of course, in the historical retail choice model, ESCOs must obtain the customer's express authorization in order to have a valid transaction. In the CCA market construct, customer data is shared with the municipality and ESCO at various stages to conduct the procurement, to send opt-out letters and then detailed information is shared to enroll the customer. By allowing customer information to be shared without customers' express authorization in a CCA, there was a heightened need for consumer protection and there was clearly a different balancing of interests than in the instant case. This difference is punctuated in the CCA DSA and the DSA being proposed here because there is no provision in the CCA DSA regarding retention of records on customer authorization. A fresh look by the Commission is warranted here.

Another obvious difference between the CCA DSA and the instant DSA is the proposal to require that ESCOs secure $10 million in cybersecurity insurance (a utility proposal that was specifically rejected by the Commission in the CCA case)[5] as well as ESCO contractors. The $10 million cybersecurity insurance requirement is not calibrated to be commensurate with the potential risk posed by transmitting the customer data. It also imposes a significant cost on ESCOs and ESCO contractors, is not widely available or readily obtainable. NEM has more detailed recommendations on the cybersecurity insurance requirement herein. For these reasons, the generic application of the CCA DSA to all ESCOs in the retail marketplace is inappropriate and should be reviewed anew by the Commission. Indeed, utilities and ESCOs have been engaging in EDI transactions to exchange customer information for nearly two decades in the regular course of conducting business in the retail marketplace.

In general, NEM recommends that the appropriate manner to formulate and adopt cybersecurity practices and processes for the retail energy marketplace is through revision to the UBP. Housing cybersecurity requirements in the UBP better ensures that all potentially affected entities (such as new market entrants or ESCO contractors as applicable) receive proper notice and are aware of their compliance obligations. The DSAs and Self-Attestation forms as proposed have terms and requirements embedded within them that will have the effect of setting precedent on many important issues, including determinations of what constitutes protected customer information; standards for information security programs; and the propriety of applying cybersecurity insurance requirements to ESCOs, to name a few. Industry standard cybersecurity policy to be embedded in a DSA and Self-Attestation form should be subject to Commission review and approval and should be maintained in the UBP. As revisions and updates to

[3] Cases 16-M-0015 and 14-M-0224, Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications, issued October 19, 2017.
[4] NEM is not aware of any pending filing by any utility with the Commission proposing the DSA that all ESCOs are being required to sign or any SAPA notice of such.
[5] Id. at 24.

cybersecurity requirements become necessary, the stakeholder process for revising the UBP can be utilized. The UBP also currently includes requirements for EDI transactions.

Notwithstanding the foregoing, NEM offers the following comments on the proposed DSAs and Self-Attestation forms. NEM also requests an extension for the Self-Attestation forms for the reasons set forth in Section II of these comments.

I. Proposed Data Service Agreements

The utilities in New York, in their role as distribution system operators, must robustly maintain and protect their grid infrastructure against cyberattacks and physical attacks. ESCOs do not own or operate delivery infrastructure networks and have discreet and limited interactions with the utilities data systems. Commission cybersecurity policy and any DSA incorporating that policy must recognize this difference in the nature of the systems to be protected and should not impose utility-scale cybersecurity requirements on ESCOs. Commission cybersecurity policy and any DSA 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. ESCOs should also be afforded a reasonable period of time to become compliant with these new requirements.

NEM's comments address the issues in the order of the provisions generally set forth within the DSAs.

Definitions

The DSAs include definitions of significant terms including "Confidential Utility Information," "Data Protection Requirements," "Data Security Incident," "Personal Data," "Sensitive Data," "Utility Data," and "Third Party Representative" that require further discussion and consideration. Issues for discussion include:

- Any definitions, and associated performance obligations, in the DSA should be in conformance with existing legal and regulatory requirements regarding personally identifiable information.[6] New York law already proscribes a process for the handling of data breaches.

[6] See NY GBL § 899-aa (1) definitions.
(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;
(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:
(1) social security number;
(2) driver's license number or non-driver identification card number; or
(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
(c) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of

- As a general overarching principle, the DSA should recognize and reflect that the customer in the retail marketplace owns its own data and can direct which entity is authorized to access and use that data.
- ESCOs own and obtain customer data received directly from the customer with consent. ESCOs also obtain data from other sources, such as marketing lists. The treatment of this information should be clearly distinguished. The "Additional Obligations" provision of the DSA only makes narrow reference to data collected by an ESCO "from customers through its website or other interactions based on those customers' interest in receiving information from other otherwise engaging with [ESCO] or its partners" not being considered to be Confidential Utility Information.
- Definitions of "Confidential Utility Information" and "Sensitive Data" should be focused on that information which is accurately characterized as such, noting that certain customer information is widely available from public sources, and that the definitions may need to be differentiated based on customer class.
- A justification enunciated for the DSA is the risk associated with sharing the status of customers participation in affordability assistance programs. This concern is simply inapplicable to ESCOs that do not serve residential customers. Moreover, as relevant for those ESCOs that do serve residential customers, a customer's status as a low income program participant is never actually conveyed to the ESCO in the EDI transaction. Rather, the enrollment transaction is rejected without revealing that information.[7]
- The definition of "Third Party Representative" should be clarified. The DSA defines it as ESCO agents "that are contractors or subcontractors." Such a broad definition could unintentionally include third party marketers operating on behalf of an ESCO, a result clearly not intended nor needed to protect the utilities' systems. In the Commission's recent Order opening the Cybersecurity Standard Proceeding for the ESCO marketplace, it was noted that discussions with Staff, utilities, and "energy service entities" had already been undertaken about the DSA. The Order defined "energy service entities" as including "ESCOs, Electronic Data Interchange (EDI) providers, and any other third party that contracts with an ESCO to communicate data between the ESCO and the utility." These are both very expansive definitions, the application of which would cast a very wide net in applying performance and/or compliance obligations. Serious consideration should be given to limiting these definitions and the application of

---

the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

[7] See Case 12-M-0476 et.al. Order Adopting Prohibition on Service to Low Income Customers by Energy Service Companies, issued December 16, 2016, at pages 19-20. See also "With respect to new enrollments, an enrollment of an APP will simply be rejected with a reason that does not identify the customer as APP." Case 12-M-0476, Order on Rehearing and Providing Clarification, issued September 19, 2016, at page 18. NEM expressly reserves and does not waive any rights, issues, or claims being adjudicated by the Court in the pending litigation concerning the moratorium on ESCO service to low income customers.

requirements and obligations to entities that pose a real risk to the utility system. Care should also be taken to ensure all of these entities have received notice of the development of the DSA and have had an opportunity to weigh in on these cybersecurity protection standards.

Third Party Compliance with all Applicable Commission Uniform Business Practices

In this Section, the ESCO signatory is required to indicate what type of entity it is and that it "expressly agrees to comply with the Commission's ESCO Uniform Business Practices ("UBP"), as they may be amended from time to time." This latter phrase is unnecessary as ESCO compliance obligations with the UBP already apply.

Customer Consent

The DSA would require ESCOs to retain records of customer consent for six years. Recordkeeping requirements should not exceed the current two-year UBP recordkeeping requirement.

Confidentiality

The DSA would restrict the processing and storage of confidential utility information to locations within the U.S. No basis has been given for restricting the location of ESCO or ESCO contractor operations, and it is an overly restrictive intrusion into ESCO businesses. Particularly if the ESCO and its contractors have satisfactorily completed the Self-Attestation form, there should be no reason to impose such a restriction. Moreover, operations in countries with robust data protection standards, such as GDPR compliant countries, should be deemed acceptable.

Exceptions Allowing Third Party to Disclose Confidential Utility Information

Subsection a. of this provision of the DSA requires ESCO "Representatives" to execute written agreements assuming direct liability to the utility for a breach associated with confidential utility information that is disclosed to it. It would be impracticable for ESCOs to get their "Representatives" to assume that type of liability. It would require the renegotiation of existing agreements with these entities, which may not be feasible.

Return/Destruction of Information

The DSA would require ESCOs to return and destroy Confidential Utility Information within ten days of a utility's written demand. There are legitimate business reasons why ESCOs need to retain customer information, such as for tax reporting purposes or to respond to an inquiry from the Commission, even after they have ceased to serve the customer. ESCOs should be permitted to retain such information subject to the obligation to securely return or destroy the information when it is commercially practicable to do so. For these purposes, it is important to have clear distinctions as to what accurately constitutes Confidential Utility Information and what does not.

Audit

The DSA would require the ESCO and its Representatives to allow the utility and regulators to audit facilities, practices and procedures associated with processing Confidential Utility Information. In general, permitting *any* business partner to have access to confidential and proprietary systems and facilities raises serious security concerns for ESCOs themselves. Audits may also violate existing agreements with other vendors and affiliates.

UBP Section 2 defines the process of PSC review of ESCO operations and need not be addressed in the DSA.

Any discussion of audits of ESCO and ESCO representative operations should address the following:

- If the ESCO or ESCO representative has developed and implemented operationally appropriate cybersecurity policies (meaning appropriate to the size and scope of the business), this should supplant the need for an audit. This could be demonstrated, for example, by:
    - Satisfactory completion of the Self-Attestation form[8] by the ESCO with officer certification; or
    - Satisfactory completion of the Self-Attestation form by the ESCO's EDI vendor; or
    - Adoption of the NIST cybersecurity security standard for its systems and facilities; or
    - Compliance with the Payment Card Industry Data Security Standard (PCI DSS)[9]; or
    - Other reasonable demonstration of operationally appropriate cybersecurity policies.

- If an audit requirement is imposed, it should be subject to the following:
    - The audit should only be performed by a qualified independent third party, agreed upon by the parties.[10]
    - The audit should only be required premised on good cause shown.
    - A documented audit process should be established.
    - The audit should not be required on an annual basis due to its time and cost-intensive nature.
    - ESCOs must be afforded a reasonable period of time to cure any deficiencies discovered in the course of an audit.

[8] This recommendation is contingent upon the final terms to be included in the Self-Attestation form.

[9] 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).

[10] Id. at 6-8 (directing that the utilities cybersecurity programs be subject to third party audit and evaluation).

- If an ESCO has been subject to audit by a utility, that ESCO should not be subjected to audit by another utility.

Data Security Incidents

The DSA defines "Data Security Incident" and includes a process for the ESCO to follow in the case of a data security incident involving confidential utility information that is processed by the ESCO or on its behalf. New York law already proscribes a process to be followed in the case of the "breach of the security of the system."[11] DSA requirements should be in conformance with these existing requirements. For instance, the requirement for an ESCO to notify a utility within twenty-four hours is unnecessarily strict and burdensome.

The utility should have a mutual obligation to notify the ESCO when the utility believes that a data security incident has taken place. This will allow the ESCO to protect its customers.

[11] NY GBL § 899-aa provides that:

2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

Cybersecurity Insurance Required

The DSA would require ESCOs to maintain cybersecurity insurance of at least $10 million per incident and that includes the utility as an additional insured. ESCO contractors are to maintain cybersecurity insurance of like amount. One of the goals expressed by the Commission for opening this proceeding is "explor[ing] whether insurance is an efficient and effective vehicle for mitigating any potential risks."[12] In this regard, NEM submits that stakeholders should be focused on the cybersecurity processes and systems that ensure the safe and secure transmission, processing, storage, and disposal of data that avoids the occurrence of data breaches in the first instance. NEM and its members are not aware of any other jurisdiction or utility that currently requires retail marketers to maintain cybersecurity insurance.[13]

The cybersecurity insurance requirement imposes a significant cost on ESCOs, estimated in the range of $70,000-100,000, and is not widely available or readily obtainable. For a company that operates multiple ESCOs or multiple brands in the New York marketplace, if each ESCO was required to maintain insurance, it would be cost prohibitive. These exorbitant costs will be passed on to consumers and will falsely make ESCO pricing appear less competitive.

A cybersecurity insurance requirement should not be imposed on the ESCO community without a thorough examination of the following:

- The blanket imposition of a $10 million insurance requirement on every ESCO and ESCO contractor has not been supported or justified by any quantifiable evidence.

- UBP Section 3 affords ESCOs with different ways of demonstrating creditworthiness. A similar approach to demonstrating cybersecurity protection should be considered here, rather than a strict cybersecurity insurance requirement. This could be demonstrated, for example, by:

    - ESCO demonstration that it has implemented cybersecurity practices that are appropriate to the size and scope of its operation. This could be demonstrated through satisfactory completion of the Self-Attestation form by the ESCO[14]; satisfactory completion of the Self-Attestation form by the ESCO's EDI vendor; compliance with the NIST cybersecurity standard; compliance with the Payment Card Industry Data Security Standard (PCI DSS); or other reasonable means of demonstrating operationally appropriate cybersecurity protection; or
    - A reasonable cybersecurity insurance requirement; or
    - Allowing the ESCO to be self-insured; or
    - Letters of credit or other similar security instrument.

- If a cybersecurity insurance requirement is imposed, it should be calibrated to the risk posed by the individual entity, rather than the blanket imposition of the $10 million

[12] Case 18-M-0376, Order Instituting Proceeding, issued June 14, 2018, page 3.
[13] The recent data security incident that prompted the instant inquiry impacted multiple states. In those states, stakeholders convened to discuss the matter, but regulatory action was not taken.
[14] This recommendation is contingent upon the final terms to be included in the Self-Attestation form.

insurance requirement on all ESCOs and their contractors. Insurance requirements should be set at a level that is commensurate with the extent of the ESCO's interaction with the utility system. The UBP creditworthiness requirements are calibrated to the risk of the individual entity, and that approach should be followed if cybersecurity insurance is required. For example, the level of insurance should incorporate considerations including:

- If an ESCO has satisfactorily completed the Self-Attestation form,[15] if the ESCO's EDI vendor satisfactorily completed the Self-Attestation form; if the ESCO is in compliance with the NIST cybersecurity standard, if the ESCO is in compliance with the PCI DSS or other operationally appropriate cybersecurity measures, then the ESCO should not be subject to the insurance requirement.
- 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.
- The extent to which an individual ESCO receives confidential data does vary. 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.

- If a cybersecurity insurance requirement is imposed, a process should be established for when and how the insurance will be drawn upon as well as a periodic process for review of the amount of the insurance required.

No Intellectual Property Rights Granted

The DSA states that the ESCO does not acquire an ownership interest in Confidential Utility Information by virtue of the agreement. Importantly, the DSA also cannot create rights to customer data, which is owned by the customer, for the utility.

Additional Obligations

The DSA would require the ESCO to "safely secure and encrypt all Confidential Utility Information during storage or transmission." The encryption of confidential data when in transit is a good business practice for ESCOs and utilities to comply with. The encryption of all utility data when it is stored in ESCO systems (i.e., hard drives and databases) would require extensive rewriting of those systems. The appropriate focus should be on the *secure* storage of utility data.

Payment

It is unclear what "Utility fees" are being referred to in this provision. This should be clarified.

[15] This recommendation is contingent upon the final terms to be included in the Self-Attestation form.

Specific Performance

The DSA preserves the utility's ability to seek specific performance and/or injunctive relief to enforce compliance with the agreement, while requiring the ESCO to waive the ability to seek a bond or other security to protect its interest (so the ESCO can protect itself in the event that injunctive relief or specific performance results in harm to the ESCO). While the preservation of the right to specific performance or injunctive relief is relatively standard, the requirement for the ESCO to waive the bonding or other security is not.

Indemnification

The indemnification provision in the DSA is broader than a standard indemnity provision. For example, it is inclusive of attorney's fees, court costs, expenses, and regulatory penalties. The indemnification provision should also be made mutual to the ESCO.

Term

The DSA does not set forth any term, rather allowing the utility to terminate on ten days prior written notice. However, it does not provide the ESCO with a reciprocal ability to terminate.

II. Comments on and Request for Extension of the Self-Attestation Form

The utilities originally provided ESCOs with Vendor Risk Assessment (VRA) forms to complete. Subsequently, the utilities devised a joint Self-Attestation of Information Security Controls, in place of the VRA. We appreciate the utilities efforts to standardize the requirements. However, we have substantive concerns with the Self-Attestation form that justify an extension to correspond with the process for consideration of the DSA.

The utilities are requiring the Self-Attestation to be signed by the end of June. However, the Self-Attestation includes material terms that are as of yet undefined such as "confidential utility information," "information security policy" and "information security program." It also includes terms and obligations that are dependent upon what is to be established as a "final" DSA. It would be premature for ESCOs to sign a binding Self-Attestation form without first knowing what the final terms of the DSA will be. It would also be premature for ESCOs to sign a binding Self Attestation form without the utilities' having first agreed to enter into a nondisclosure agreement. A NDA is necessary because of the confidential and proprietary nature of the information being sought in the Self-Attestation form from the ESCOs. Accordingly, the deadline for executing the Self-Attestation form should be extended and aligned to correspond with the process for consideration of the DSA.

In addition, the Whereas Clause of the document has combined all of the utilities in the execution of the single document. This is problematic as it appears the utilities would be in a position to act collectively to remove an ESCO from the market based on the ESCO's completion of the form. The Self-Attestation form also includes an audit requirement that is duplicative of the audit requirement that is set forth in the DSA and is unnecessary.

III. Conclusion

NEM appreciates the opportunity to submit these comments on the proposed DSA and Self-Attestation form and the Commission's development of industrywide cybersecurity practices and processes. We look forward to future opportunities for stakeholder dialogue on this subject.

NEM also respectfully requests that the deadline for executing the Self-Attestation form be extended and aligned to correspond with the process for consideration of the DSA.

Finally, NEM notes that the stakeholders agreed to schedule a follow up meeting after the submission of comments and the utilities opportunity for review. NEM previously scheduled its Summer Executive Committee Meeting for July 25-26th. NEM respectfully requests that the follow up meeting not be scheduled on those dates so as to permit NEM and its members to participate fully in the discussions.

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: June 28, 2018.