STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data	**)**	**Case 20-M-0082**
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	**)**	**Case 18-M-0376**

Comments of Family Energy, Inc.

Family Energy, Inc.[1] [hereinafter "Family"] hereby submits comments on the "Joint Utilities' Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates," [hereinafter "JU Petition"] dated May 3, 2022. Notice of the JU Petition was filed in the May 25, 2022, New York State Register. These comments are filed pursuant to the State Register Notice. In the JU Petition, they propose to revise six existing requirements and add three new requirements to the Self-Attestation (SA) provision of the Data Security Agreement (DSA) considered in Case 18-M-0376. The JU Petition also proposes a governance process to be utilized for SA review and for the purpose of providing recommendations for further SA updates. The JU request that the Petition be addressed during the Commission's September session.

Family recommends that the proposed SA revisions and additions discussed herein be rejected or modified as explained herein. The DSA, including the SA, was recently approved by the Commission in 2019.[2] In the Petition, the JU are proposing significant changes to the SA without

[1] Family Energy, Inc. is a Business Corporation, incorporated in New York, and authorized by the Commission to serve electric and natural gas customers as an Energy Service Company.
[2] Cases 18-M-0376, 15-M-0180 and 98-M-1343, Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, issued October 17, 2019 [hereinafter "2019 Order"].

explanation or justification besides a generalized assertion that it is necessary for cybersecurity purposes. Certain proposals being made in the instant JU Petition, regarding the defined term "Confidential Customer Utility Information" and the exemption for emails from the encryption in transit requirement, reflect proposals that were previously evaluated in the 2019 Order and expressly rejected. Another proposal, regarding the maintenance of a data inventory, was raised in a different JU filing, but no Commission Order has been issued approving such proposal. Family suggests that the Commission's 2019 Order correctly decided a number of complex and interrelated issues and that the JU have offered no justification to change it now.

The Commission recognized in the 2019 Order that cybersecurity standards should be appropriate to the entity. The Commission specifically rejected the idea that ESCOs and third-party utility vendors should be subject to the same cybersecurity standards.[3] Here, the JU are raising examples of cybersecurity standards adopted in other industries that are not comparable as a purported justification for modifying the SA requirements for ESCOs. The JU maintain that their proposed updates reflect NIST standards incorporated in the Transportation Security Agency's (TSA's) recent Security Directive and the Department of Defense's (DOD's) Cyber Maturity Model Certification process.[4] The JU fail to explain how TSA and DOD cybersecurity standards and the

[3] The Commission reasoned that,

> Addressing first the comments asserting that ESE should not be treated the same as utility vendors, the Commission agrees. However, the Petition is clear that though the Joint Utilities would like the ESEs to have more protections, they are not being treated like distribution utility vendors. Vendor requirements are established via contractual terms and agreements that are based upon the vendor having high level of access directly into the utility IT systems, possibly behind firewalls. ESEs will not have this higher level of access and have a direct relationship with the customer, not implementing a program or service for the utility. ***The necessary cybersecurity and privacy requirements for ESEs will not be established based upon the risk associated with vendor access but on the risk associated with the ESEs restricted access to utility IT systems and/or data***. (emphasis added).

2019 Order at 34.

[4] JU Petition at 7-8.

entities these standards apply to are analogous here to the ESCO-utility relationship and the level of ESCO access to utility information systems and data.

Family also recommends that any governance process for SA review and revisions should include the ESCO community in an active role. As was made evident during the discussions and filings regarding the original DSA, seeking ESCO input and engagement up-front in the process of developing cybersecurity standards is critical to ensuring that the standards are reasonably achievable, properly reflective of technological realities and constraints, and appropriate to the type and size of the subject entity and its activities.

Indeed, Family suggests that all of the proposed modifications and additions to the SA in JU Petition should be reviewed in a stakeholder collaborative prior to the Commission rendering a decision in order to permit an opportunity for meaningful and thoughtful dialogue between the JU and ESCOs as to the scope and purpose of the proposed changes and to allow ESCOs to thoroughly articulate concerns about implementation. To the extent that any of the proposed changes to the SA are adopted, ESCOs should have a sufficient period of time to implement those changes in their own systems.

Family Energy will address each of the specific proposed changes to the SA below in accordance with the numbering utilized in the JU Petition.

Cybersecurity Protection #3

> *Current SA language with proposed additions indicated* - Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis. **Authentication and password controls align with NIST 800-63B: Digital Identity Guidelines**. (proposed new language in bold).

NIST 800-63B is a lengthy document, the implementation of which would entail significant and substantive changes. The JU should clarify which portions of the NIST 800-63B standard are proposed to be made applicable to ESCOs, and the JU should also provide a detailed explanation of the reasons therefor beyond a generalized assertion that it is needed to enhance cybersecurity protections.

Cybersecurity Protection #7

> *Current SA language* – All Confidential Customer Utility Information is encrypted in transit utilizing industry best practice encryption methods, except that Confidential Information does not need to be encrypted during email communications.
>
> *Proposed SA language* – Encrypt all Confidential Customer and Non-Public Utility Information in transit using encryption methods compliant with NIST cryptographic standards and guidelines.

There are two significant changes proposed to be made here. The first is a changed reference to the defined term in the DSA, "Confidential Customer Utility Information," to a term that is not defined in the DSA, "Confidential Customer and Non-Public Utility Information." As a general matter, it is unclear how ESCOs can be expected to be compliant with an undefined term. More importantly, the term "Confidential Customer Utility Information" as used in the DSA was carefully crafted by stakeholders and subsequently approved by the Commission in the 2019

Order.[5] The definition of "Confidential Customer Utility Information" as set forth in the current DSA is as follows,

> "Confidential Customer Utility Information" means information that Utility is: (A) required by the UBP at Section 4: Customer information (C)(2), (3) or UBP DERS at Section 2C: Customer Data (C)(2), to provide to ESE or (B) any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party is such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

Of particular note, when the Commission approved the definition in 2019, it changed the name of the term from "Confidential Utility Information" to "Confidential Customer Utility Information." In making this change, the Commission reasoned that,

> while the Commission agrees with the scope of this definition, the term "Confidential Utility Information" does not adequately represent the data itself. This term advances the idea that this is utility information when that is not the case. Instead, this is customer information that is held by the utility. For these reasons, the term "Confidential Utility Information" shall be replaced with the term "Confidential Customer Utility Information." This will better reflect that this is the customer's utility data, not data "owned" by the utility.[6]

It is unclear if the JU's proposed change to the nomenclature of the term to "Confidential Customer and Non-Public Utility Information" is intended to undo this very important Commission finding

[5] 2019 Order at p. 47.
[6] Id.

related to a customer's ownership of its own data or make any other substantive change to the definition.

The term "Confidential Customer Utility Information" also includes important exclusions for generally available information, information otherwise known on a non-confidential basis, information obtained from another source on a non-confidential basis, independently-developed information and information provided by the customer with consent that the customer expressly agrees is public information. It is unclear if by proposing to change the nomenclature of the defined term to "Confidential Customer and Non-Public Utility Information," whether and how the existing exceptions would potentially be changed.

The JU have offered no explanation as to why the defined term "Confidential Customer Utility Information" should be changed, and Family recommends that the current existing nomenclature and substantive definition should remain unchanged in Cybersecurity Protection #7 and as used elsewhere in the SA.

The second change proposed to be made to Cybersecurity Protection #7 is to remove the exemption for emails from the encryption in transit requirement. The current SA does not require that emails be encrypted in transit. This appropriately reflects the reality that when ESCOs correspond with their customers by email that the customer will not have encryption/decryption technology, nor should there be a reasonable expectation that the customer would have that technology. The Commission also addressed this issue in the 2019 Order as follows,

> Communicating via encrypted emails require the sender and recipient to have a pre-existing relationship with software to encrypt and decrypt the content of emails. Additionally, many ESEs utilize email to communicate with their customers, a vast majority of which will not have the ability to encrypt emails or receive encrypted emails from their chosen ESE. The Joint Utilities exclude email from the electronic

> communications with ESEs that trigger the need for a DSA. That same exception should be applied to the encryption in transit requirement. Thus, encryption of Confidential Customer Utility Information will not be required for email communications. This modification will allow ESEs to effectively communicate with customers and other entities without first establishing a process for mutual encryption and decryption.[7]

The JU have not demonstrated any changed circumstances from that recognized by the Commission in 2019 in setting forth the email exemption to the encryption in transit requirement for Confidential Customer Utility Information, and indeed there is none. The email exemption is a reasonable accommodation for ESCO and customer communications. Accordingly, this proposed change to Cybersecurity Protection #7 should be rejected.

Cybersecurity Protection #8

> *Current SA language* – All Confidential Customer Utility Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.
>
> *Proposed SA language* - Encrypt all Confidential Customer and Non-Public Utility Information at rest using encryption methods compliant with NIST cryptographic standards and guidelines, or is otherwise physically secured.

Family reiterates its objection to the use of the undefined term "Confidential Customer and Non-Public Utility Information" in reference to Cybersecurity Protection #8 for the same reasons as explained above in reference to Cybersecurity Protection #7. Family agrees with the language in the proposal that would permit ESCOs to continue to have the option to encrypt the Confidential Customer Utility Information *or* to ensure the information is otherwise physically secured.

[7] 2019 Order at p. 52.

Cybersecurity Protection #13

> *Current SA language with proposed additions indicated* - Employee background screening**, including criminal background checks,** occurs prior to the granting of access to Confidential Customer Utility Information. (proposed new language in bold).

Family submits that employee background screening is a sufficient measure to take prior to granting the employee access to Confidential Customer Utility Information. This is especially true given the nature of the information to be exchanged,[8] which does not include sensitive customer credit card or banking information. A criminal background check would be excessive under the circumstances.

Additionally, from a legal and practical perspective, employers may be prohibited by locally applicable employment law from retroactively performing a criminal background check after an employee is hired unless that employee expressly consents. Accordingly, if the criminal background check is incorporated into Cybersecurity Protection #13, it should only be applied prospectively to new employee hires.

Cybersecurity Protection #15

> *Current SA language with proposed additions indicated* - Access to Confidential Customer Utility Information is revoked **within 24 hours** when no longer required, or if employees separate from the ESE or Third Party Representative. (proposed new language in bold).

[8] "Confidential Customer Utility Information" as currently defined in the DSA includes information that the utility is required by the UBP at Section 4: Customer Information (C)(2) and (3) to provide to the ESCO; or any other information provided to the ESCO by the utility and marked confidential at the time of disclosure. Neither UBP Section 4.C.2, the Customer Contact Information Set, or 4.C.3., the Billing Determinant Information Set, include customer credit card or banking information.

Family suggests that this proposal should be modified so that employee access is revoked "within 24 hours of a regular business day." This modification would account for the fact that an employee may separate from service on a Friday evening, which could delay the process for revoking access credentials by appropriate personnel over the weekend until the commencement of the next regular business day.

Cybersecurity Protection #16

> *Proposed SA language (no current SA provision)* – Developing and maintaining a data inventory that an ESE can use to catalog its data and location.

The JU propose that ESEs develop and maintain a data inventory. This proposal mirrors the proposal the JU filed regarding the Data Access Framework Matrix in Case 20-M-0082.[9] Noteworthy in this regard is the fact that the Commission has not issued an Order either approving or denying the JU's prior proposal. Also noteworthy is the JU admission that "[t]his item is a work in progress for the Joint Utilities, as it is for many entities."[10] In other words, the JU do not currently adhere to their proposed modification to the SA, but they are asking the Commission to require it with respect to ESCOs. It is simply unfair and unreasonable to require ESCOs to adhere to a standard (possibly as soon as the September 2022 session) to which the utility proponents do not currently adhere. Moreover, more detail should be provided as to what constitutes a data inventory so that ESCOs can comply with any such requirement. For example, "data" is a broad term that should be meaningfully defined to provide context and limits. Likewise, it is unclear

[9] Case 20-M-0082, Joint Utilities' Comments on Data Access Framework Matrix, filed August 20, 2021, at p. 4.
[10] JU Petition at note 34.

how broadly the data inventory is intended to reach – possibly to include computers, servers, file cabinets or a subset of those limited by the type of data being stored.

Cybersecurity Protection #17

> *Proposed SA language (no current SA provision)* – Organization communications (i.e., information transmitted or received by organizational systems) are monitored, controlled and protected at the external boundaries and key internal boundaries of the information systems. Sub-networks for publicly accessible system components are physically or logically separated from internal networks. Management of devices use encrypted sessions.

Family submits that the language of proposed Cybersecurity Protection #17 appears overly broad as though it is intended to function as a catchall provision. For example, "monitored, controlled and protected" is quite general terminology. Family recommends that clarification of the purpose and intended scope of this language be provided and that appropriately tailored protections be developed to meet those specific needs.

Cybersecurity Protection #18

> *Proposed SA language (no current SA provision)* – Physical access to organizational information systems, equipment, and the respective operating environments is limited to authorized individuals. Physical security controls include the following:
> - Visitors are escorted and their activity is monitored
> - Audit logs of physical access are maintained
> - Physical access devices are controlled and managed

It is unclear how this proposed provision will apply when "organizational information systems" are not located in a physical location but rather are cloud-hosted. Family suggests that if an ESCO's servers are in the cloud, that an alternative to this proposed provision should be to accept the SOC II Type 2 Audit Report as a means of compliance.

Governance Committee

The JU propose that the Commission establish a Governance Committee for the purpose of providing regular review and updates to the SA. The Governance Committee would consist of up to five JU members and up to five Staff members, that are cybersecurity subject matter experts. The JU propose that an Advisory working group be formed, comprised of ESEs and NYSERDA, to provide the Governance Committee with feedback on proposed recommendations for updates to the SA.

Family agrees that there is a need for on-going industry engagement on cybersecurity issues. Family submits that it is critical that ESCOs be substantively engaged up-front in any recommendations to change the SA. Otherwise, the Committee will essentially be making proposals in a vacuum without an understanding of how the modifications will affect ESCO operations, whether the changes are technologically achievable, or whether a less burdensome measure could be adopted that would achieve the desired result. It will be a far more efficient use of stakeholder time and resources for ESCOs to be able to provide input early on when modifications to the SA are being considered, rather than to delay engaging ESCOs in evaluating proposed SA modifications until filed with the Commission for review and approval. Limiting ESCO engagement on proposed modifications to the SA to reacting and responding to a JU filing once made at the Commission, limits the opportunity for a meaningful exchange of ideas and concerns. It also potentially delays the process of updating the SA, to the extent that ESCOs identify issues that were not contemplated by the JU at the time of filing.

Conclusion

For the foregoing reasons, Family recommends that the proposed SA revisions and additions be rejected or modified consistent with the suggestions set forth in these Comments. Family also recommends that ESCOs be actively engaged up-front in discussions on cybersecurity standards and potential proposed modifications. All of the proposed modifications and additions to the SA in the JU Petition should be reviewed in a stakeholder collaborative prior to the Commission rendering a decision. To the extent that any of the SA modifications proposed by the JU are adopted, the ESCOs must have a reasonable amount of time to implement any new cybersecurity obligations.

Respectfully submitted,

s/Stacey Rantala

Stacey Rantala
Associate Director, Government & Regulatory Affairs
Family Energy, Inc.
P.O. Box 967
Buffalo, NY 14240-0967
PH: 646-720-1038
srantala@sfeenergy.com

Dated: July 25, 2022.