advanced energy management alliance

PO Box 65491
Washington, DC 20035

p 202.580.8284
e info@aem-alliance.org

aem-alliance.org

December 18, 2018

CORRECTED VERSION--VIA ELECTRONIC MAIL

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

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

Dear Secretary Burgess:

Advanced Energy Management Alliance (AEMA) is submitting comments on the Data Security Agreements and Self-Attestation Forms proposed by the Joint Utilities of New York to apply to DER Suppliers under the Distributed Energy Resource Suppliers Uniform Business Practices. The attached document includes a summary and explanation of our recommendations.

We appreciate your consideration of these comments. Please do not hesitate to contact me at 202-524-8832 should you have any questions or require additional information regarding this filing.

Respectfully submitted,

Katherine Hamilton
Executive Director, AEMA

Cc: Parties to Case

BEFORE THE
STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

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

COMMENTS OF ADVANCED ENERGY MANAGEMENT ALLIANCE ON DATA SECURITY AGREEMENTS AND SELF-ATTESTATION FORMS FOR DISTRIBUTED ENERGY RESOURCE SUPPLIERS

Advanced Energy Management Alliance ("AEMA")[1] respectfully submits these comments pursuant to the "business to business" process underway in Case Number 18-M-0376 and the request by the Department of Public Service staff ("DPS" or "Commission"), Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation, and Rochester Gas and Electric Corporation (together, the "JU") for Distributed Energy Resource Suppliers ("DER Suppliers") to provide written comments on the Data Security Agreements and Self Attestation Forms ("DSA or DSAs") in the stakeholder meeting held on November 14, 2018 concerning the applicability of the DSA to DER Suppliers.

[1] AEMA is an alliance of providers and supporters of distributed energy resources united to overcome barriers to nationwide use of distributed energy resources, including demand response and advanced energy management, for an environmentally preferable and more reliable grid. We advocate for policies that empower and compensate customers to manage their energy usage to make the electric grid more efficient, more reliable, more environmentally friendly, and less expensive.

Introduction and Background

AEMA is a trade association under Section 501(c)(6) of the Federal tax code whose members include national distributed energy resource companies and advanced energy management service and technology providers, including demand response ("DR") providers, as well as some of the nation's largest demand response and distributed energy resources ("DER" or "DERs"). AEMA members participate in the New York Independent System Operator's ("NYISO") Special Case Resources ("SCR") program and engage in the New York State Utilities demand response programs like Commercial System Relief Program ("CSRP"), Distribution Load Relief Program ("DLRP"), and Direct Load Control ("DLC"). To facilitate participation in these programs, AEMA members rely on access to customer data provided by the utility. These comments represent the collective consensus of AEMA as an organization, although they do not necessarily represent the individual positions of the full diversity of AEMA member companies.

Executive Summary

AEMA thanks DPS staff for recognizing in their staff report[2] the differences that exist between ESCOs and EDI providers (herein "energy services entities" or "ESEs") and DER Suppliers, and for initiating a separate process to review applicability of the DSAs to DER Suppliers as AEMA recommended in previous comments.[3] DER Suppliers require different data points and interact with the JU differently than ESEs. The scale and

[2] Department of Public Service Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry, filed in 18-M-0376 on September 24, 2018, pp.7-8.
[3] Comments of Advanced Energy Management Alliance on Data Security Agreements, filed in 18-M-0376 on July 2, 2018, p.4.

scope of customer data collected by DER Suppliers varies significantly from ESEs, as do the classes of customers served. AEMA appreciates the opportunity to engage collaboratively with DPS staff and the JUs on how to amend these DSAs to create the best data privacy and security framework for the customers of DER Suppliers.

AEMA and its members take cybersecurity risks and protection of confidential information seriously and share in the interests that the DPS staff and JU have in ensuring that utility customer data is protected. However, AEMA is concerned about the scope of the DSAs and their applicability to DER Suppliers. The provisions within the DSAs, while based upon NIST standards, appear to go far beyond the scope and contain terms to which few, if any, DER Suppliers would be willing to agree. Imposing overly-onerous cybersecurity rules upon DER Suppliers could drive companies out of the New York market and impede entry, stifling innovation and reducing competition. Given the importance of the DER Supplier community to delivering clean energy solutions to customers that reduce usage and save money for all New York ratepayers, this outcome would be highly detrimental to the ambitious targets of the Reforming the Energy Vision ("REV") initiatives.

AEMA applauds the Commission's recent expansion of these targets and their recognition of concerns over the impacts that impediments to accessing data may have. In the Commission Order recently issued on Energy Efficiency Targets, the Commission recognized the importance of access to data by DER Suppliers and called for a new comprehensive proceeding to address data access and for utilities to accelerate their

implementations of GBC platforms.[4] AEMA and its members look forward to participating in this forthcoming proceeding. AEMA cautions, however, that if issues with the DSAs remain unresolved and the JU push forward with requiring DSAs to be executed by DER Suppliers in advance of the 2019 DLRP and CSRP season, a direct result could be a significant decrease in participation in these programs.

Given the importance of data privacy and security issues, the importance of DER Suppliers to New York's ambitious REV goals, and the unique nature of DER Suppliers, AEMA makes the following recommendations to Staff on the JU's proposed DSAs:

- DPS staff should continue to ensure that these proceedings are proactively communicated to the full ESE and DER Supplier community in order to facilitate robust industry participation;
- DER Suppliers that engage only with Commercial and Industrial ("C&I") customers should not be required to sign the DSA. Large C&I customers are sophisticated, have experience with data privacy and security issues, and therefore need less protection and pose less risk to utilities than mass market customers. DER Suppliers may still be required to submit signed Self-Attestations to utilities. This would be consistent with prior Commission action in its DER Oversight Order;[5]
- Certain terms in the DSA impose untenable risks and costs to DER Suppliers without improving the privacy and security of customer data.

[4] Order Adopting Accelerated Energy Efficiency Targets, issued in 18-M-0084 on December 13, 2018, pp.41-44.
[5] Order Establishing Oversight Framework and UBPs for DER Suppliers.

This includes the indemnification clause, audit clause, and lack of a limitation on liability clause, among others. AEMA has suggested redlined edits (see Appendix A) that would correct these flaws. These edits would do nothing to erode the protections that customers are afforded by these DSAs, but would ensure that DER Suppliers can continue to operate in a manageable business risk environment; and

- If significant areas of disagreement remain between parties, the Commission may need to rule on such issues to provide fairness and certainty to the process.

AEMA looks forward to continued engagement on these issues to develop robust and appropriate data safeguard standards for New York. We expand on these recommendations below.

A. Process Concerns

While AEMA appreciates and supports the business to business collaborative effort facilitated by DPS staff between the JU and DER Suppliers, AEMA is concerned that not all stakeholders have been made aware of the applicable timeframes for participating in this process. While the notice of the November 14th stakeholder meeting[6] was cross-posted in case numbers 18-M-0376, 18-M-0084, and 15-M-0180, participation by DER Suppliers in the meeting did not seem to encompass the broad community of companies and organizations that could be impacted by this process. Requests were made by several stakeholders present during the meeting to increase messaging within the

[6] Notice of Stakeholder Meeting, filed in 18-M-0376, 18-M-0084, and 15-M-0180 on October 23, 2018.

Document and Matter Management System ("DMM"), perhaps by expanding the notice list to additional case numbers. To date, there has been no subsequent notice on the DSA for DER Suppliers, and no additional notice of the request for comments or other next steps discussed during the meeting have been posted in the aforementioned matter numbers nor on the DPS' webpage for Vendor Risk Assessment – Data Security Agreement Matters.[7] AEMA recommends that DPS staff provide notice more broadly to ensure all entities potentially impacted by this process have the opportunity to participate within the stakeholder process.

AEMA thanks the DPS for creating a separate website[8] to host content related to the business to business process. However, AEMA is concerned that there is a lack of continuity between which documents are stored on the website and in the DMM for 18-M-0376. While the organization of the site is helpful to segment out information (including the addition of a DER-specific subsection), AEMA thinks it would be helpful to include the dates of when each document is posted to help provide further context when reviewing the materials.

Finally, AEMA is concerned about the lack of Commission approval of the DSAs. Should parties fail to reach a consensus through the business to business collaborative process on issues of contention, AEMA respectfully requests that the Commission rule on such matters to provide clarity and certainty to all parties. The last workshop exposed

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

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

significant disagreement between the JUs and other stakeholders on nearly every point, and AEMA is concerned about a lack of reasonable negotiation between the parties. If parties are unable to bridge the gaps in the business to business process, AEMA is hopeful that these issues will be more thoroughly addressed in the forthcoming proceeding on comprehensive data rules concerning DER Suppliers.[9]

B. Applicability to DER Suppliers

AEMA urges the Commission to consider the applicability of the DSAs to DER Suppliers that deal only with Large C&I Customers.[10] As the Commission noted in its Order Establishing Oversight Framework and UBPs for DER Suppliers ("DER Oversight Order"), these customers are "substantially more sophisticated and often retain energy experts, attorneys, and other professionals to assist their procurement of DER products and services" than mass market customers.[11] The Commission found that it was therefore appropriate to exempt Large Customers, and the DER Suppliers that serve them, from the more prescriptive oversight rules.

The Commission is right to be concerned about protecting the data privacy and security of mass market customers, who may lack the knowledge and resources to do so themselves. However, large C&I customers are inherently different. These customers have significant business and financial interest in safeguarding their data and ensuring the companies they work with have sufficient data protections in place. For C&I customers,

[9] Order Adopting Accelerated Energy Efficiency Targets, issued in 18-M-0084 on December 13, 2018, pp.41-44.
[10] Defined, consistent with the VDER Phase One Order and the Order Establishing Oversight Framework and UBPs for DER Suppliers, a "customers that are within a jurisdictional utility's non-residential demand-based or mandatory hourly pricing (MHP) service classification".
[11] Order Establishing Oversight Framework and UBPs for DER Suppliers, page 21.

data privacy and security are therefore daily parts of their business, which may not be the case for many mass market customers. Furthermore, C&I businesses are subject to a variety of national laws related to data privacy, security, and protection, including the Federal Trade Commission Act (FTC Act), the Financial Services Modernization Act (Gramm-Leach-Bliley Act), and the Health Insurance Portability and Accountability Act (HIPAA). Any multi-state company is furthermore subject to a multitude of state laws, including California's S.B. 570, A.B. 964, A.B. 1541, and the recently passed California Consumer Privacy Act of 2018. As a result, these companies have a sophisticated understanding of data privacy and security and, by necessity, frameworks and procedures in place to ensure the continued safety and confidentiality of their data.

The Commission should therefore recognize that large C&I customers have the ability to self-regulate in this space, and should not institute redundant data security standards for the companies that serve them. DER Suppliers doing business with C&I customers already have robust privacy and security standards in place, just like the C&I customers that they serve. The C&I businesses themselves will often require them to do so. Furthermore, in the event of a data security incident or breach, the contractual terms between DER Suppliers and their C&I customers should be sufficient to cover the protections, rights, responsibilities, and implications of any such breach, with these contracts being developed by knowledgeable attorneys. The proposed DSA will therefore provide little value to C&I customers who can already protect themselves. **AEMA urges the Commission to take action consistent with its findings in its DER Oversight**

Order and exempt Large Customers, and their DER Suppliers, from the requirement to sign DSAs.

We note that the risks to utilities of DER Suppliers handling C&I customers' data is relatively minor as well. Much of the customer data the DER Suppliers receive is received directly from the customer. All of it is received with customers' express consent. In the event of a data security incident, C&I customers are extremely unlikely to sue their utility as a result of a DER Supplier's negligence, unless the utility itself was also negligent. Furthermore, the relatively small number of C&I customers relative to mass market customers means fewer touch points with utility systems, further reducing the risk they may face.[12] There is therefore no need to require DER Suppliers to sign the DSAs as the protection of C&I customer data, and proper data handling and security practices by DER Suppliers, are already established.

Finally, we recognize that some level of oversight for C&I-focused DER Suppliers may be warranted given the growing importance of data privacy and security throughout the energy industry. As noted previously, AEMA is supportive of companies maintaining robust controls and procedures to safeguard customer data and protect against data security incidents. We therefore suggest that all DER Suppliers could be required to submit the Self-Attestation to utilities, to provide assurances that they have appropriate controls in place and to provide a forum for collaborative discussions on privacy and security practices, if such discussions are warranted. However, only DER

[12] While the JUs have characterized this risk as catastrophic, they ignore the fact that risk is a combination of impact and likelihood. The impact of a data security incident can certainly be large, but the likelihood of such an event caused directly by the transfer of data between a utility and DER supplier is exceedingly small. AEMA believes this risk has been grossly misrepresented by the JUs and would urge the Commission to focus, first and foremost, on establishing a framework that safeguards customer data.

Suppliers that deal with mass-market customers would be required to sign the full DSA. This type of action would be consistent with the Commission's action in its DER Oversight Order. Note also that this recommendation is contingent on AEMA's concerns regarding the DSA and Self-Attestation, outlined below and in Appendix A, being resolved.

C. Specific Feedback on DSA Documents

AEMA is concerned about several aspects of the DSA and their applicability to DER Suppliers. While AEMA appreciates that the JU has worked to come to agreement on a standard document that can be utilized with each individual utility, AEMA has specific feedback regarding the DSAs that, if not addressed, would make signing these agreements untenable to DER Suppliers. Below AEMA lays out our overarching and specific concerns with pertinent sections of the DSAs. Additionally, redline edits to the DSAs that accompany these comments has been included in Appendix A.

a. Specific Comments to the DSA

i. Section 4 – Customer Consent

The Customer Consent section, along with the UBP-DERS Section 2C(B), conflicts with how GBC works today. Under GBC, the utility holds a customer's consent, not the DER Supplier, although DER Suppliers would obtain authorization from the customer through contractual language or other consent mechanisms. AEMA members would be willing to work with the JU and DPS staff on the JU members' GBC implementation to alter the process to comply with the current DSA language.

ii. Section 5 – Provision of Information

The open-ended language in subsection B of section 5 could require parties to enroll in additional security assessments that they do not currently perform, resulting in additional costs which ESEs would be required to cover. The provision of information should be limited to the Self-Attestation that is currently included as a part of the DSA.

iii. Section 6 – Confidentiality

The Confidentiality section, as drafted, is an overly-strict liability standard to comply with. ESEs and utilities should only be held liable if they fail to undertake commercially-reasonable or appropriate data security practices. Please see the attached redlines to this effect.

iv. Section 9 – Audit

There is already a process for taking corrective actions subject to utility approval following a data security incident outlined in Section 11. Having an outside audit occur at the same time would be disruptive, duplicative, and counterproductive. AEMA's members would strongly object to being subject to utility audits if they already maintain a SOC II audit program (or equivalent); it is not a process we would agree to in any collaborative, business to business negotiation. Additionally, these audit provisions may be difficult for new market entrants and could be a significant barrier due to the disruption to their business.

v. Section 11 – Data Security Incidents

With regards to the notification of a Data Security Incident, our redlines, attached, seek to align with Europe's General Data Protection Regulations ("GDPR").[13] It may take more than 48 hours to reasonably determine whether an Incident has taken place and to understand and effectively communicate the potential impacts. We believe this is a reasonable compromise supported by strong international standards.

vi. Section 12 – Cybersecurity Insurance Required

The cybersecurity insurance requirement of $5MM per incident is overly-onerous and AEMA believes this requirement will serve as a barrier to entry for new market participants seeking to obtain utility customer data. The costs of obtaining a policy may be too steep to provide cost-effective solutions to their customers and the market. AEMA suggests a tiered approach to the cybersecurity insurance requirement that is reflective of a company's size and of the risk posed by the amount of data it intends to hold.

vii. Section 14 – Additional Obligations

The goal of this section of the DSA should be to ensure the continued and effective privacy protection of customers. However, this clause as written could hinder DER Suppliers in their ability to innovate and develop insights from aggregated customer data to improve services to customers.

viii. Section 16 – Indemnification

The DSA should be about protecting customer data and privacy in the event of data security incidents. The indemnification clause as written would pass untenable risks

[13] See GDPR website: https://eugdpr.org

onto ESEs without any improvement to customer data protections because of the lack of a liability standard. AEMA members would not sign a contract with such an indemnification clause as currently written; being required to do so would likely force DER Suppliers, including AEMA members, to reconsider whether to enter or continue operating in the state. The inclusion of such language in the final DSA would be indicative of a completely unbalanced negotiation in which the voice of the DER Supplier community is silenced to the detriment of future business and innovation in the State of New York.

ix. Insertion of a new Section 17 – Limitation of Liability

AEMA proposes inserting a new section 17, titled "Limitation on Liability," that would effectively limit an ESE's aggregate liability to a value that should not exceed $1MM. This limitation on liability is crucial to create a strong data privacy framework that protects customer data while ensuring that ESEs operate in a manageable risk environment.

x. Self-Attestation of Information Security Controls

The Incident Response Procedure (second Requirement) notification time has been changed from 48 to 72 hours. As noted above in AEMA's comments on the Data Security Incidents section, this is the standard notice period outlined in the GDPR. Please reference our earlier comments for further justification for this requested change.

The storage location of Confidential Utility Information (10th Requirement) has been changed to a more flexible definition denoting that the manner in which the data are

stored and the location where data are stored comply with all applicable federal, state, and local laws and regulations.

D. Conclusion

AEMA appreciates the opportunity to submit comments for consideration by the Commission, DPS staff, and the JU and respectfully requests that these parties accept these comments and adopt recommendations made herein.

Respectfully Submitted,

Katherine Hamilton, Executive Director
Advanced Energy Management Alliance
www.aem-alliance.org
1200 18th Street, NW, Suite 700
Washington, DC 20036

Appendix A:
Draft Redline Edits to Data Security Agreement and Self-Attestation Form
[see following pages]

DATA SECURITY AGREEMENT

This Data Security Agreement ("Agreement") effective _____, is made and entered into this _____ day of _____ , 20___ by and between ("Utility") and _____, an Energy Service Entity ("ESE") with offices at _____ ; and together with Utility the ("Parties" and each, individually, a "Party").

RECITALS

WHEREAS, ESE desires to have access to certain utility customer information, either customer-specific or aggregated customer information, or the New York State Public Commission ("Commission") has ordered Utility to provide to ESE customer information; and

WHEREAS, ESE has obtained consent from all customers from whom the ESE intends to obtain information from Utility; and

WHEREAS, Energy Services Company ("ESCO"), Direct Customer or Distributed Energy Resource ("DER") Supplier may utilize a third party to fulfill its Service obligations, including but not limited to, Electronic Data Interchange ("EDI") communications with Utility; and

WHEREAS, ESCO, Direct Customer or DER Supplier ("DERS") utilization of a third party provider does not relieve ESCO, Direct Customer or DERS of their transactional obligation such that they must ensure that the third party provider must comply with all ESCO, Direct Customer or DERS obligations; and

WHEREAS, Utility and ESE also desire to enter into this Agreement to establish, among other things, the full scope of ESE's obligations of security and confidentiality with respect to the Confidential Information in a manner consistent with the rules and regulations of the Commission and requirements of Utility; and

NOW, THEREFORE, in consideration of the premises and of the covenants herein contained, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, hereby agree as follows:

1. Definitions.

a. "Confidential ESE Information" means information that ESE is: (A) required by the Uniform Business Practices ("UBP") or DERS UBP ("UBP DERS") to receive from the end use customer and provide to Utility to enroll the customer or (B) any other information provided by ESE to Utility and marked confidential by the ESE, 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 if 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.

b. "Confidential 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, to provide to ESCO, Direct Customer or DERS 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 if 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.

c. "Confidential Information" means, collectively, Confidential Utility Information or Confidential ESE Information.

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

e. "Data Security Incident" means a situation when Utility or ESE reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Information; (B) the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Confidential Information, or Private Information as defined by GBL § 899-aa, computer systems, network and devices used by a business; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Information, or (D) any material breach of any Data Protection

Requirements in relation to the Processing of Confidential Information, including by any current or former Representatives.

f. "DER Supplier" or "DERS" has the meaning set forth in the UBP DERS approved by the Commission and as it may be amended from time to time, which is "[a] supplier of one or more DERs that participates in a Commission authorized and/or utility or DSP-operated program or market. DERS may choose to provide DERs as standalone products or services, or may choose to bundle them with energy commodity. CDG Providers and On-Site Mass Market DG Providers are included within the definition of DERS. Entities which sell both DERs and energy commodity are both DERS and ESCOs."

g. "Direct Customer" has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is "An entity that purchases and schedules delivery of electricity or natural gas for its own consumption and not for resale. A customer with an aggregated minimum peak connected load of 1 MW to a designated zonal service point qualifies for direct purchase and scheduling of electricity provided the customer complies with NYISO requirements. A customer with annual usage of a minimum of 3,500 dekatherms of natural gas at a single service point qualifies for direct purchase and scheduling of natural gas."

h. "ESCO" has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is "an entity eligible to sell electricity and/or natural gas to end-use customers using the transmission or distribution system of a utility."

i. "ESE" shall have the meaning set forth in the Recitals and for the avoidance of doubt, includes but is not limited to ESCOs, Direct Customers, DERS and contractors of such entities with which Utility electronically exchanges data other than by email and any other entities with which Utility electronically exchanges data other than by email or by a publicly available portal.

j. "PSC" or "Commission" shall have the meaning attributed to it in the Recitals.

k. "Processing" (including its cognate, "process") means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed using or upon Confidential Information or Utility Data, whether it be by physical, automatic or electronic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, use, transfer, hosting, maintenance, handling, retrieval, consultation, use, disclosure, dissemination, exfiltration, taking, removing, copying, processing, making available, alignment, combination, blocking, deletion, erasure, or destruction.

l. "Third-Party Representatives" or "Representatives" means those agents acting on behalf of ESCOs, Direct Customers, or DERS that are contractors or subcontractors and that store, transmit or process Confidential Utility

Information. For the avoidance of doubt, Third-Party Representatives do not include ESEs and their members, directors, officers or employees who need to know Confidential Utility Information for the purposes of providing Services.

m. "Services" mean any assistance in the competitive markets provided by ESEs to end use customers or ESCOs, Direct Customers or DERS that also require interaction with a Utility, including but not limited to the electronic exchange of information with a Utility, and must be provided in accordance with the UBP or UBP DERS.

n. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of ESE.

2. **Scope of the Agreement.** This Agreement shall govern security practices of ESEs that have electronic communications, other than email, with the Utility and security practices that apply to all Confidential Utility Information disclosed to ESE or to which ESE is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by ESE (or it its Representatives) and Confidential ESE Information. No financial information, other than billing information, will be provided pursuant to this Agreement. If any information is inadvertently sent to ESE or Utility, ESE or Utility will immediately notify the Utility/ESE and destroy any such information in the appropriate manner.

3. **ESE Compliance with all Applicable Commission Uniform Business Practices.** The Parties agree that the Commission's UBP and UBP DERS set forth rules governing the protection of Confidential Information and electronic exchange of information between the Parties, including but not limited to EDI.

_____ESCO, Direct Customer or DERS utilizes a Third-Party Representative as a vendor, agent or other entity to provide electronic exchange of information, other than by email, with Utility ESE and will require Third-Party Representative to abide by the applicable UBP or UBP DERS.

4. **Customer Consent.** The Parties agree that the UBP and UBP DERS govern an ESE's obligation to obtain informed consent from all customers about whom ESE requests data from Utility. The ESE agrees to comply with the UBP and UBP DERS on customer consent and the Utility's tariffs regarding customer consent.

5. **Provision of Information.** Utility agrees to provide to ESE or its Representatives, certain Confidential Utility Information, as requested, provided that: (A) ESE and its Representatives are in compliance with the terms of this Agreement in all material respects; (B) if required by Utility, ESE has provided and has required its Representatives to provide, to the satisfaction of Utility any Vendor Product/Service Security Assessments or self–attestations (attached hereto as Exhibit A) ~~or such other risk assessment forms as Utility may require from time to time ("Assessment")~~ and ESE will comply with the Utility Assessment requirements as approved by the Utility; (C) ESE (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as

detailed in the Assessment acceptable to Utility to protect system security and Confidential Utility Information; and; (D) ESE complies and shall require its Third-Party Representatives who process Confidential Information to comply with Utility's Assessment requirements as approved by the Utility. Provided the foregoing prerequisites have been satisfied, ESE shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to ESE. Nothing in this Agreement will be interpreted or construed as granting either Party any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right or any right to assert any lien over or right to withhold from the other Party any Data and/or Confidential Information of the other Party. Utility will comply with the security requirements set forth in its Assessment.

6. Confidentiality. ESE shall: (A) undertake commercially-reasonable efforts to hold all Confidential Utility Information in ~~strict~~ confidence pursuant to the UBP or UBP DERS and Commission's orders; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Utility Information to any Third-Party Representatives, or affiliates, except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential Utility Information; (E) store Confidential Utility Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential Utility Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as ESE employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (G) to the extent required by the Utility, each Representative with a need to know the Confidential Utility Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, Utility shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential Utility Information are being observed and ESE shall be obligated to promptly provide Utility with the requested assurances.

Utility shall: (A) hold all Confidential ESE Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential ESE Information to any other person or entity except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential ESE Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential ESE Information; (E) store Confidential ESE Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential ESE Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential ESE Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (G) to the extent required by ESE, each Representative with

a need to know the Confidential ESE Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, ESE shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential ESE Information are being observed and Utility shall be obligated to promptly provide ESE with the requested assurances.

This Section 6 supersedes prior non-disclosure agreements between the Parties pertaining to Confidential Information.

7. Exceptions Allowing ESE to Disclose Confidential Utility Information.

a. Disclosure to Representatives. Notwithstanding the provisions of Section 6 herein, the Parties may disclose Confidential Information to their Third-Party Representatives who have a legitimate need to know or use such Confidential Information for the purposes of providing Services in accordance with the UBP and UBP DERS, provided that each such Third-Party Representative first: (A) is advised by the disclosing Party of the sensitive and confidential nature of such Confidential Information; (B) agrees to comply with the provisions of this Agreement, provided that with respect to Third-Party Representatives and this subsection (B), such Third-Party Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Third-Party Representatives were a Party/ESE; and (C) signs the Third-Party Representative Agreement. All such written Agreements with Third-Party Representatives shall include direct liability for the Third-Party Representatives towards Utility/ESE for breach thereof by the Third-Party Representatives, and a copy of such Agreement and each Third-Party Representative Agreement shall be made available to Utility/ESE upon request. Notwithstanding the foregoing, the Parties shall be liable for any act or omission of a Third-Party Representative, including without limitation, those acts or omissions that would constitute a breach of this Agreement.

b. Disclosure if Legally Compelled. Notwithstanding anything herein, in the event that a Party or any of its Third-Party Representatives receives notice that it has, will, or may become compelled, pursuant to applicable law or regulation or legal process to disclose any Confidential Information (whether by receipt of oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, other similar processes, or otherwise), that Party shall, except to the extent prohibited by law, within one (1) business day, notify the other Party, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, the Parties shall have the right to consult and the Parties will cooperate, in advance of any disclosure, to undertake any lawfully permissible steps to reduce and/or minimize the extent of Confidential Information that must be disclosed. The Parties shall also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Information that must be disclosed. In any event, the Party and its Third-Party Representatives shall disclose only such Confidential Information which they are advised by legal

counsel that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Party) and the Party and its Third-Party Representatives shall use all reasonable efforts to ensure that all Confidential Information that is so disclosed will be accorded confidential treatment.

8. Return/Destruction of Information. Within thirty (30) days after Utility's written demand, ESE shall (and shall cause its Third-Party Representatives to) cease to access and Process Confidential Utility Information and shall at the Utility's option:
(A) return such Confidential Utility Information to Utility in such manner, format, and timeframe as reasonably requested by Utility or, if not so directed by Utility,
(B) shred, permanently erase and delete, degauss or otherwise modify so as to make unreadable, unreconstructible and indecipherable ("Destroy") all copies of all Confidential Utility Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Utility Information) that has come into ESE's or its Third-Party Representatives' possession, including Destroying Confidential Utility Information from all systems, records, archives, and backups of ESE and its Third-Party Representatives, and all subsequent access, use, and Processing of the Confidential Utility Information by ESE and its Third-Party Representatives shall cease provided any items required to be maintained by governmental administrative rule or law or necessary for legitimate business or legal needs will not be destroyed until permitted and will remain subject to confidentiality during the retention period. ESE agrees that upon a customer revocation of consent, ESE warrants that it will no longer access through Utility Confidential Utility Information and that it will Destroy any Confidential Utility Information in its or its Third-Party Representative's possession. Notwithstanding the foregoing, ESE and its Third-Party Representatives shall not be obligated to erase Confidential Utility Information contained in an archived computer system backup maintained in accordance with their respective security or disaster recovery procedures, provided that ESE and its Third-Party Representatives shall: (1) not have experienced an actual Data Security Incident; (2) maintain Data Security Protections to limit access to or recovery of Confidential Utility Information from such computer backup system and; (3) keep all such Confidential Utility Information confidential in accordance with this Agreement. ESE shall, upon request, certify to Utility that the destruction by ESE and its Third-Party Representatives required by this Section has occurred by (A) having a duly authorized officer of ESE complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Third-Party Representatives and maintaining them on file. Compliance with this Section 8 shall not relieve ESE from compliance with the other provisions of this Agreement. The written demand to Destroy or return Confidential Utility Information pursuant to this Section may occur if the ESE has been decertified pursuant to the UBP or UBP DERS, the Utility has been notified of a potential or actual Data Security Incident and Utility has a reasonable belief of potential ongoing harm or the Confidential Utility Information has been held for a period in excess of its retention period. The obligations under this Section shall survive any expiration of termination of this

Agreement. Subject to applicable federal, state and local laws, rules, regulations and orders, at ESE's written demand and termination of electronic exchange of data with Utility, Utility will Destroy or return, at ESE's option, Confidential ESE Information.

9. **Audit.** Upon thirty (30) days notice to ESE, ESE shall, and shall require its Third-Party Representatives to permit Utility, its auditors, designated representatives, to audit and inspect, at Utility's sole expense (except as otherwise provided in this Agreement), and provided that the audit may occur no more often than once per twelve (12) month period (unless otherwise required by Utility's regulators). The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Utility Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESE's security practices and procedures, facilities, resources, plans, procedures, and books and records relating to the privacy and security of Confidential Utility Information. Such audit rights shall be limited to verifying ESE's compliance with this Agreement, including all applicable Data Protection Requirements. If the ESE provides a SOC II report or its equivalent to the Utility, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to the Utility at ESE's sole expense, within one hundred eighty (180) days, no Utility audit is necessary~~ absent a Data Security Incident~~. Any audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement. Utility shall provide ESE with a report of its findings as a result of any audit carried out by or on behalf of Utility. ESE shall, within thirty (30) days, or within a reasonable time period agreed upon in writing between the ESE and Utility, correct any deficiencies identified by Utility, and provide the SOC II audit report or its equivalent or the report produced by the independent auditor to the Utility and provide a report regarding the timing and correction of identified deficiencies to the Utility.

10. **Investigation.** Upon notice to ESE, ESE shall assist and support Utility in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Utility Information Processed by ESE on behalf of Utility. Such assistance shall be at Utility's sole expense, except where such investigation was required due to the acts or omissions of ESE or its Representatives, in which case such assistance shall be at ESE's sole expense.

11. **Data Security Incidents.** ESE is responsible for any and all Data Security Incidents involving Confidential Utility Information that is Processed by, or on behalf of, ESE. ESE shall notify Utility in writing immediately (and in any event within ~~forty~~seventy~~-eight~~ two (~~48~~72) hours) whenever ESE reasonably believes that there has been a Data Security Incident. After providing such notice, ESE will investigate the Data Security Incident, and immediately take all necessary steps to eliminate or contain any exposure of Confidential Utility Information and keep Utility advised of the status of such Data Security Incident and all matters related thereto. ESE further agrees to provide, at ESE's sole cost: (1) reasonable assistance and cooperation requested by Utility and/or Utility's designated representatives, in the

furtherance of any correction, remediation, or investigation of any such Data Security Incident; (2) and/or the mitigation of any damage, including any notification required by law or ~~that~~ Utility's ~~may determine appropriate~~ regulatory authority to send to individuals impacted or potentially impacted by the Data Security Incident; and (3) and/or the provision of any credit reporting service required by law or ~~that~~ Utility's ~~deems appropriate~~ regulatory authority to provide to such individuals. In addition, within thirty (30) days of confirmation of a Data Security Incident, ESE shall develop and execute a plan, subject to Utility's approval, which approval will not be unreasonably withheld, that reduces the likelihood of a recurrence of such Data Security Incident. ESE agrees that Utility may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a Data Security Incident occurs and it has a reasonable belief of potential ongoing harm. Any suspension made by Utility pursuant to this paragraph 11 will be temporary, lasting until the Data Security Incident has ended, the ESE security has been restored to the reasonable satisfaction of the Utility so that Utility IT systems and Confidential Utility Information are safe and the ESE is capable of maintaining adequate security once electronic communication resumes. Actions made pursuant to this paragraph, including a suspension will be made, or subject to dispute resolution and appeal as applicable, pursuant to the UBP or UBP DERS processes as approved by the Commission.

12. **Cybersecurity Insurance Required.** Commencing by December 1, 2018, ESE shall carry and maintain Cybersecurity insurance in an amount of no less than $5,000,000 per incident. Utility will maintain at least $5,000,000 of Cybersecurity insurance.

13. **No Intellectual Property Rights Granted.** Nothing in this Agreement shall be construed as granting or conferring any rights, by license, or otherwise, expressly, implicitly, or otherwise, under any patents, copyrights, trade secrets, or other intellectual property rights of Utility, and ESE shall acquire no ownership interest in the Confidential Utility Information. No rights or obligations other than those expressly stated herein shall be implied from this Agreement.

14. **Additional Obligations.**

a. ESE shall not create or maintain data which are derivative of Confidential Utility Information that could expose customers' Personally Identifiable Information (PII) except for the purpose of performing its obligations under this Agreement or as authorized by the UBP or UBP DERS. For purposes of this Agreement, the following shall not be considered Confidential Utility Information or a derivative thereof: (i) any customer contracts, customer invoices, or any other documents created by ESE that reference estimated or actual measured customer usage information, which ESE needs to maintain for any tax, financial reporting or other legitimate business purposes consistent with the UBP or UBP DERS; and (ii) Data collected by ESE from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESE or its partners.

b. ESE shall comply with all applicable privacy and security laws to which it is subject, including without limitation all applicable Data Protection Requirements and not, by act or omission, place Utility in violation of any privacy or security law known by ESE to be applicable to Utility.

c. ESE shall have in place appropriate and reasonable processes and systems, including an Information Security Program, defined as having completed an accepted Attestation as reasonably determined by the Utility in its discretion, to protect the security of Confidential Utility Information and prevent a Data Security Incident, including, without limitation, a breach resulting from or arising out of ESE's internal use, processing, or other transmission of Confidential Utility Information, whether between or among ESE's Third-Party Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of ESE, including without limitation Third-Party Representatives. The Utility's determination is subject to the dispute resolution process under the UBP or UBP DERS.

d. ESE and Utility shall safely secure or encrypt during storage and encrypt during transmission all Confidential Information.

e. ESE shall establish policies and procedures to provide reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of a Data Security Incident involving Confidential Utility Information Processed by ESE to the extent such request, complaint or other communication relates to ESE's Processing of such individual's Confidential Utility Information.

f. ESE shall establish policies and procedures to provide all reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Confidential Utility Information, data theft, or other unauthorized release of Confidential Utility Information, disclosure of Confidential Utility Information, or misuse of Confidential Utility Information to the extent such request, complaint or other communication relates to ESE's accessing or Processing of such Confidential Utility Information.

g. ESE will not process Confidential Utility Information outside of the United States or Canada absent a written agreement with Utility. For the avoidance of doubt, Confidential Utility Information stored in the United States or Canada, or other countries as agreed upon in writing will be maintained in a secure fashion at a secure location pursuant to the terms and conditions of this Agreement.

15. Specific Performance. The Parties acknowledge that disclosure or misuse of Confidential Utility Information in violation of this Agreement may result in irreparable harm to Utility, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore Utility shall be entitled to specific performance and/or injunctive relief to

enforce compliance with the provisions of this Agreement. Utility's right to such relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Agreement, at law or in equity, including monetary damages, the right to terminate this Agreement for breach and the right to suspend in accordance with the UBP and UBP DERS the provision or Processing of Confidential Utility Information hereunder. ESE agrees to waive any requirement for the securing or posting of any bond or other security in connection with Utility obtaining any such injunctive or other equitable relief.

16. **Indemnification.** To the fullest extent permitted by law, ESE shall indemnify and hold Utility, its affiliates, and their respective officers, directors, trustees, shareholders, employees, and agents, harmless from and against any and all loss, cost, damage, or expense of every kind and nature (including, without limitation, penalties imposed by the Commission or other regulatory authority or under any Data Protection Requirements, court costs, expenses, and reasonable attorneys' fees) arising out of, relating to, or resulting from, in whole or in part, the breach or non-compliance with this Agreement by ESE or any of its Third-Party Representatives ~~except~~ to the extent that the loss, cost, damage or expense is caused by the negligence, gross negligence or willful misconduct of ~~Utility~~ESE.

~~16.~~17. **Limitation on Liability.** "ESE's aggregate liability hereunder is limited to direct actual damages as the sole and exclusive remedy, and total damages under the Agreement shall not exceed one million ($1,000,000) dollars. In no event shall either Party, its parent, officers, directors, partners, shareholders, employees or affiliates, or any contractor or subcontractor or its employees or affiliates, be liable to the other Party for special, indirect, exemplary, punitive, incidental or consequential damages of any nature whatsoever connected with or resulting from the Solutions or from performance or non-performance of obligations under the Agreement, including without limitation, damages or claims in the nature of lost revenue, income or profits, loss of use, or cost of capital, irrespective of whether such damages are reasonably foreseeable and irrespective of whether such claims are based upon negligence, strict liability contract, operation of law or otherwise."

~~17.~~18. **Notices.** With the exception of notices or correspondence relating to potential or pending disclosure under legal compulsion, all notices and other correspondence hereunder shall be sent by first class mail, by personal delivery, or by a nationally recognized courier service. Notices or correspondences relating to potential or pending disclosure under legal compulsion shall be sent by means of Express Mail through the U.S. Postal Service or other nationally recognized courier service which provides for scheduled delivery no later than the business day following the transmittal of the notice or correspondence and which provides for confirmation of delivery. All notices and correspondence shall be in writing and addressed as follows:

If to ESE, to:

ESE Name:
Name of Contact:
Address:

Phone:
Email:

If to Utility, to:

Utility Name:
Name of Contact:
Address:
Phone:
Email:

A Party may change the address or addressee for notices and other correspondence to it hereunder by notifying the other Party by written notice given pursuant hereto.

18. **Term and Termination.** This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated in accordance with the provisions of the service agreement, if any, between the Parties or the UBP or UBP DERS and upon not less than thirty (30) days' prior written notice specifying the effective date of termination, provided, however, that any expiration or termination shall not affect the respective obligations or rights of the Parties arising under this Agreement prior to the effective date of termination. Utility may terminate this Agreement if the ESE is decertified under the UBP or DER UBP, has not served customers for two (2) years, or has not had electronic communication, other than by email, with Utility for one (1) year. Further, Utility may terminate this Agreement immediately upon notice to ESE in the event of a material breach hereof by ESE or its Third-Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 14, 16, and 24 shall be a material breach hereof. Upon the expiration or termination hereof, neither ESE nor its Third-Party Representatives shall have any further right to Process Confidential Utility Information or Customer Information and shall immediately comply with its obligations under Section 8 and the Utility shall not have the right to process Confidential ESE Information and shall immediately comply with its obligations under Section 8.

19. **Consent to Jurisdiction; Selection of Forum**. ESE irrevocably submits to the jurisdiction of the Commission and courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Agreement. ESE agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ESE at the address for ESE pursuant to Section 11 hereof and that such service shall be deemed sufficient even under circumstances where, apart from this Section, there would be no jurisdictional basis for such service. ESE agrees that service of process on it may also be made in any manner permitted by law. ESE consents to the selection of the New York State and United States courts within _____ County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement. If the event involves all of the Utilities jurisdiction will be in Albany County, New York.

20. **Governing Law.** This Agreement shall be interpreted and the rights and obligations of the Parties determined in accordance with the laws of the State of New York, without recourse to such state's choice of law rules.

21. **Survival.** The obligations of ESE under this Agreement shall continue for so long as ESE and/or ESE's Third-Party Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all Agreements between ESE and Utility have expired or been terminated.

22. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall together constitute

one and the same instrument. Copies of this Agreement and copies of signatures on this Agreement, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.

23. **Amendments; Waivers.** Except as directed by the Commission, this Agreement may not be amended or modified except if set forth in writing signed by the Party against whom enforcement is sought to be effective. No forbearance by any Party to require performance of any provisions of this Agreement shall constitute or be deemed a waiver of such provision or the right thereafter to enforce it. Any waiver shall be effective only if in writing and signed by an authorized representative of the Party making such waiver and only with respect to the particular event to which it specifically refers.

24. **Assignment.** This Agreement (and the Utility's or ESE's obligations hereunder) may not be assigned by Utility, ESE or Third Party Representatives without the prior written consent of the non-assigning Party, and any purported assignment without such consent shall be void. Consent will not be unreasonably withheld.

25. **Severability.** Any provision of this Agreement which is determined by any court or regulatory body having jurisdiction over this Agreement to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

26. **Entire Agreement.** This Agreement (including any Exhibits hereto) constitutes the entire Agreement between the Parties with respect to the subject matter hereof and any prior or contemporaneous oral or written Agreements or understandings with respect to such subject matter are merged herein. This Agreement may not be amended without the written Agreement of the Parties.

27. **No Third-Party Beneficiaries.** This Agreement is solely for the benefit of, and shall be binding solely upon, the Parties and their respective agents, successors, and permitted assigns. This Agreement is not intended to benefit and shall not be for the benefit of any party other than the Parties and the indemnified parties named herein, and no other party shall have any right, claim, or action as a result of this Agreement.

28. **Force Majeure.** No Party shall be liable for any failure to perform its obligations in connection with this Agreement, where such failure results from any act of God or governmental action or order or other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure) which prevents such Party from performing under this Agreement and which such Party is unable to prevent or overcome after the exercise of reasonable diligence. For the avoidance of doubt a Data Security Incident is not a force majeure event.

29. **Relationship of the Parties.** Utility and ESE expressly agree they are acting as independent contractors and under no circumstances shall any of the employees

of one Party be deemed the employees of the other for any purpose. Except as expressly authorized herein, this Agreement shall not be construed as authority for either Party to act for the other Party in any agency or other capacity, or to make commitments of any kind for the account of or on behalf of the other.

30. Construction. This Agreement shall be construed as to its fair meaning and not strictly for or against any party.

31. Binding Effect. No portion of this Agreement is binding upon a Party until it is executed on behalf of that Party in the space provided below and delivered to the other Party. Prior to such execution and delivery, neither the submission, exchange, return, discussion, nor the negotiation of this document, whether or not this document is then designated as a "draft" document, shall have any binding effect on a Party.

[signature page follows]

IN WITNESS WHEREOF, the Parties have executed and delivered this Agreement as of the date first above written.

UTILITY	**ESE**
By: _____	By:
Name:_____	Name:
Title:	Title:

EXHIBIT A

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

Each Utility, for itself only, represents that for all information received from Third Party in response or pursuant to this Self-Attestation that is marked CONFIDENTIAL by Third Party (Confidential Self-Attestation Information) Utility shall: (A) hold such Confidential Self-Attestation Information in strict confidence; (B) not disclose such Confidential Self-Attestation Information to any other person or entity; (C) not Process such Confidential Self-Attestation Information outside of the United States or Canada; (D) not Process such Confidential Self-Attestation Information for any purpose other than to assess the adequate security of Third party pursuant to this Self-Attestation and to work with Third party to permit it to achieve adequate security if it has not already done so; (E) limit reproduction of such Confidential Self-Attestation Information; (F) store such Confidential Self-Attestation Information in a secure fashion and in accordance with all relevant laws and regulations at a secure location ~~in the United States or Canada~~ that is not accessible to any person or entity not authorized to receive such Confidential Self-Attestation Information under the provisions hereof; (G) otherwise use at least the same degree of care to avoid publication or dissemination of such Confidential Self-Attestation Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care.

The Requirements to complete the Self-Attestation are as follows (check all that apply to Third Party's computing environment, leave blank all that do not apply to Third Party's computing environment. For items that do not apply. If there are plans to address items that do not currently apply within the next 12 months, place an asterisk in the blank and the month/year the requirement is projected to apply to the Third Party's computing environment), comments regarding plans for compliance are encouraged:

This SELF-ATTESTATION OF INFORMATION SECURITY CONTROLS ("Attestation"), is made as of this _____ day of_____ , 20___ by _____ , a third party ("Third Party") to Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation (together, the New York State Joint Utilities or "JU").

WHEREAS, Third Party desires to retain access to certain Confidential Utility Information[1] (as defined in this Data Security Agreement), Third Party must THEREFORE self-attest to Third Party's compliance with the Information Security Control Requirements ("Requirements") as listed herein. Third Party acknowledges that non-compliance with any of the Requirements may result in the termination of utility data access as per the discretion of any of the JU, individually as a Utility or collectively, in whole or part, for its or their system(s). Any termination process will proceed pursuant to the Uniform Business Practices or Distributed Energy Resources Uniform Business Practices.

_____ An Information Security Policy is implemented across the Third Party corporation which includes officer level approval.

_____ An Incident Response Procedure is implemented that includes notification within ~~48~~ 72 hours of knowledge of a potential incident alerting utilities when Confidential Utility Information is potentially exposed, or of any other potential security breach.

_____ Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis.

_____ Multi-factor authentication is used for all remote administrative access, including, but not limited to, access to production environments.

_____ All production systems are properly maintained and updated to include security patches on a periodic basis. Where a critical alert is raised, time is of the essence, and patches will be applied as soon as practicable.

_____ Antivirus software is installed on all servers and workstations and is maintained with up-to-date signatures.

_____ All Confidential Utility Information is encrypted in transit utilizing industry best practice encryption methods.

All Confidential Utility Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.

[1] "Confidential Utility Information" means, collectively, aggregated and customer -specific information that Utility is: (A) required by the Uniform Business Practices ("UBP") at Section 4: Customer information(C)(2), (3) or Distributed Energy Provider ("DER") UBP at Section 2C: Customer data, to provide to ESCO, Direct Customer or DER Supplier and or (B) any other Data provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, or (C) a Utility's operations and/or systems, including but not limited to log-in credentials, 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 if 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.

_____ It is prohibited to store Confidential Utility Information on any mobile forms of storage media, including, but not limited to, laptop PCs, mobile phones, portable backup storage media, and external hard drives, unless the storage media or data is encrypted.

_____ All Confidential Utility Information is stored in a manner and location that complies with all applicable federal, state, and local laws and regulations ~~the United States or Canada only, including, but not limited to, cloud~~

_____ Third Party monitors and alerts their network for anomalous cyber activity on a 24/7 basis.

_____ Security awareness training is provided to all personnel with access to Confidential Utility Information.

_____ Employee background screening occurs prior to the granting of access to Confidential Utility Information.

_____ Replication of Confidential Utility Information to non-company assets, systems, or locations is prohibited.

_____ Access to Confidential Utility Information is revoked when no longer required, or if employees separate from the Third Party.

Additionally, the attestation of the following item is requested, but is NOT part of the Requirements:

_____ Third Party maintains an up-to-date SOC II Type 2 Audit Report, or security controls audit report.

IN WITNESS WHEREOF, Third Party has delivered accurate information for this Attestation as of the date first above written.

Signature: _____

Name: _____

Title: _____

Date: _____

EXHIBIT B

THIRD-PARTY REPRESENTATIVE AGREEMENT

This Third-Party Agreement to be provided to the Utility upon request.

I, _____, have read the Agreement between _____ , ("Company") and _____ , ("Utility") dated _____ __, 20__ (the "Agreement") and agree to the terms and conditions contained therein. My duties and responsibilities on behalf of _____ require me to have access to the Confidential Information disclosed by Utility to the ESE pursuant to the Agreement.

_____ _____

Signature Date