COUCH WHITE, LLP
COUNSELORS AND ATTORNEYS AT LAW

Couch White, LLP
540 Broadway
P.O. Box 22222
Albany, New York 12201-2222
(518) 426-4600

Amanda De Vito Trinsey
Partner
Direct Dial: (518) 320-3432
Telecopier: (518) 426-0376
email: adevito@couchwhite.com

June 22, 2018

VIA ELECTRONIC FILING

Hon. Kathleen H. Burgess
Secretary to the Commission
New York State Public Service Commission
Albany, NY 12223-1350

Re: Case 18-M-0376 – Proceeding on the Motion of the Commission Regarding Security Protocols and Protections in the Energy Market Place
Comments of NextEra Energy Services New York, LLC on Data Security Addendum

Dear Secretary Burgess:

NextEra Energy Services New York, LLC ("NextEra") is an energy services company ("ESCO") operating throughout the State of New York, and in 13 other States and the District of Columbia. NextEra takes the issue of data security very seriously and is committed to making sure its customers' data is appropriately protected. NextEra is ready to assist and work together with the State, the Utilities[1] and other interested stakeholders to fairly, reasonably, and swiftly address conditions that may compromise the security of customer data.

The process for developing and implementing appropriate data security protections is critical and must be conducted in a deliberate and measured way to avoid unintended consequences to customers, the Utilities, NextEra, or other ESCOs. Accordingly, and in response to the requests from Department of Public Service Staff ("Staff") and the Utilities for feedback on the proposed Data Security Addendum ("DSA"), NextEra provides these comments. NextEra also offers a mark-up of the DSA that contains appropriate and balanced terms to help advance the discussion of this matter. Going forward, NextEra recommends that this process follow the rules and procedures of the Public Service Commission ("Commission"); inasmuch as this matter implicates multiple actions and directives of the Commission, it would not be appropriate for the Utilities to unilaterally dictate the terms of the DSA.

[1] As used herein, the term "Utilities" means and includes 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.

The Commission appears to agree with this assertion. Last week, it issued an *Order Instituting Proceeding on Motion of the Commission Regarding Cyber Protocols* which supported the informal "business-to-business" review and comment process, yet preserved its role to review and decide "issues that cannot be properly resolved in that forum."[2] Given the linkage between this matter and the new proceeding, NextEra respectfully submits these comments for consideration in Case 18-M-0376 as well.

As noted above, NextEra offers the attached recommended changes to the DSA and the Self-Attestation to help move the process forward. Providing specific language for consideration by the Commission, Staff, Utilities, ESCOs, and other interested stakeholders should avoid abstract or unfocused discussions and assist in narrowing and resolving any disputes over the terms. The goal, which NextEra believes is shared by the Utilities, ESCOs, and Staff, is to develop a standard agreement and process that all stakeholders, and the regulator, can support.

I. Administrative Procedure and Violation of the UBP

As a preliminary matter, NextEra submits that the procedure being employed by the Utilities and Staff in advancing the DSA violates the Commission's established Uniform Business Practices ("UBP"). Over the past several months, NextEra received emails from the Utilities demanding that it and all other ESCOs execute a utility-drafted DSA and Vendor Risk Assessment ("VRA") by a specified date, or risk suspension of the processing of the ESCO's electronic data interchange ("EDI") transactions. Pursuant to Section 2.F.1.a of the UBP, a distribution utility may discontinue an ESCO's participation in retail access due to the ESCO's "[f]ailure to act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice." In order to initiate such a discontinuance process, the distribution utility must send a non-EDI discontinuance notice by overnight mail and verified receipt to the ESCO and Staff.

Additionally, UBP Section 2.F.3 states that the notice shall contain the following information:

a. The reason, cure period, if any, and effective date for the discontinuance;

b. A statement that the distribution utility shall notify the ESCO's customers of the discontinuance if the ESCO fails to correct the deficiency described in the notice within

[2] Case 18-M-0376, Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, Order Instituting Proceeding, (issued June 14, 2018), p. 3 ("Instituting Order").

the cure period, unless the Department directs the distribution utility to stop the discontinuance process;

c. Notification that the distribution utility may suspend the ESCO's right to enroll customers until correction of the deficiency; and

d. Notice that the correction of the deficiency within the cure period, or a Department directive, will end the discontinuance process.

The unilateral demands and threats presented by the Utilities do not comply with the above requirements of the UBP, and the Utilities do not have authority outside the UBP to cease processing ESCO EDI transactions.

Based on discussions with the Utilities at the May 31, 2018 stakeholder meeting ("May 31 Meeting"), it appears that the origin for this very expedited process was an incident that occurred with an EDI provider in March 2018. While that incident was problematic and identified the need for proper protocols for protecting customer data, it did not justify bypassing the Commission's rules and procedures or making threats to improperly interfere with ESCOs' legitimate rights and businesses. Moreover, pursuant to Section 8.B.2 of the UBP, even if that incident could be considered to have created an emergency situation justifying immediate resolution, the Utilities must file a formal dispute resolution request with the Secretary and provide a copy of the request to all involved parties and Staff. Importantly, that Section mandates that "[t]he request shall describe in detail the emergency situation requiring expedited resolution, state in detail the facts of the dispute, and, to the extent known, set forth the positions of the parties."

To date, NextEra is not aware of any dispute resolution request submitted by any Utility with respect to this matter. The UBP is equally applicable to the Utilities and ESCOs. Failure to follow these steps is a violation of the UBP.

II. The Commission Should Control This Process

Subsequent to receiving the DSA and VRA and associated improper threats from the Utilities, ESCOs brought this matter to Staff's attention, which resulted in the May 31 Meeting. The message conveyed at the meeting was that the Utilities were approaching this situation from a statewide application perspective and would be developing a unified and streamlined VRA that an ESCO could complete and send to all Utilities in the State. The Utilities were clear that they do not want to address data security on a piecemeal basis with each individual ESCO.

While some ESCOs asked for more time to review and develop comments, and for the schedule, generally, to be extended with respect to executing the DSA, at the May 31 Meeting the Utilities agreed only to provide a three-week limited comment period to accept feedback on the draft DSA and VRA. Under standard Commission practice, it is the Commission, or the

Administrative Law Judge, that establishes comment periods and otherwise sets the rules for each matter. Neither the Public Service Law, the Commission's regulations and rules, any Commission Order, or the UBP have delegated authority to the Utilities to set the deadlines and rules for this matter, or to allow the Utilities to unilaterally impose the DSA and VRA on the ESCOs. It is therefore imperative that the Commission step in to protect the rights and interests of the ESCOs conducting business in New York and the millions of New York consumers who have chosen an ESCO as their preferred electricity supplier.[3]

On or about June 8, 2018, the Utilities circulated another email to ESCOs, which replaced the VRA with a Self-Attestation form. Unlike the VRA (which was simply a survey), the Self-Attestation is a vague document that requires each ESCO to attest that "best practice" controls are in place without defining what those best practices are or referencing sources from which the best practices could be identified. The Self-Attestation inexplicably contains many of the same concepts that are included in the DSA, and it gives the Utility the sole discretion to determine whether the ESCO is in "non-compliance" with any of the requirements included and terminate the ESCO's data access. No parameters or guidelines were offered to govern how such compliance determinations are made, and the proposal contains no right of appeal of such determinations by an ESCO.

These provisions are inconsistent with the UBP, and they arguably violate the ESCOs' rights to due process (applicable here because the Utilities apparently are seeking to act as agents of the Commission since the Utilities have no independent termination authority under these circumstances). These improper demands and actions require the Commission to intervene to protect the rights of ESCOs and New York consumers who have freely exercised their right to choose their energy suppliers.

The Utilities further required, with Staff's support, that ESCOs must sign and return the Self-Attestations by June 30, 2018. Substitution of the VRA with the Self-Attestation was a significant change from the Utilities' prior position and is not consistent with the statements that were made at the May 31 Meeting. Moreover, the accelerated time period to review and sign the Self-Attestations comes concurrently with the parties' already condensed time for reviewing and commenting on the DSA.

NextEra objects to the Self-Attestation document in its entirety. Having a company share its information security practices with third parties – and identifying what security practices are and are not used – will only increase the risk of consumer data being compromised. Moreover,

---

[3] As a related point, NextEra notes that the Instituting Order erroneously stated (at p. 3) that this deadline was "agreed to by all parties." The three-week deadline was set by the Utilities over the ESCOs' collective objections and in disregard for requests for additional time to properly respond to the proposed documents.

NextEra objects to any requirement that the Self-Attestation be executed before the DSA is finalized. The Utilities have not offered any rational basis or legitimate explanation justifying the need for executed Self-Attestations by June 30, and NextEra respectfully submits that there is none.[4] This is a further reason why Commission intervention is needed.

III. Content of the DSA

NextEra offers the following comments on the DSA to underscore its concerns with the provisions proposed by the Utilities. In addition to these suggested revisions, there are several significant issues that need to be resolved : (i) determining what constitutes "Confidential Utility Information"; (ii) establishing what data security issues the Joint Utilities' actions are intended to prevent/solve; (iii) establishing a cause/effect and limitation of liability with respect to inclusion of any indemnification provision; (iv) revising the DSA to include mutual data protections for the Utilities and ESCOs; and (v) distinguishing the CCA DSA from an ESCO DSA.

First and foremost, there appears to be a fundamental disagreement between the Utilities and the ESCOs as to what is considered to be "Confidential Utility Information." NextEra receives most all of its customer-specific information (including utility account number) directly from its customers, independent of the Utilities.

It is standard practice in confidentiality or non-disclosure agreements in the utility industry, and in Commission proceedings, that certain types of information are excluded from the definition of "Confidential Information." The very common exclusions are: (a) information which is or becomes publicly available (except in violation of a confidentiality agreement); (b) information which is or becomes available on a non-confidential basis from a source which is not prohibited from disclosing such information pursuant to a legal, contractual or fiduciary obligation; (c) information which a party can establish was legally in its possession prior to disclosure by the other party; or (d) information which a party can establish was developed by or for it independently of any action by the other party. Here, under standard practice the information NextEra obtains directly from its customers should be considered information excluded from the definition of Confidential Utility Information in a confidentiality agreement between it and a Utility.

Determining what constitutes Confidential Utility Information for purposes of developing data security protocols and procedures for parties interacting with the Utilities is a threshold issue that must be resolved before this process can move forward. To the extent that there is disagreement amongst the ESCOs and the Utilities as to what constitutes Confidential Utility Information, consistent with the Instituting Order, such issue should be referred to the

[4] To be clear, NextEra agrees that all parties – ESCOs and Utilities alike – should use appropriate and reasonable safeguards for customer data, but there first needs to be a determination of what is appropriate and reasonable.

Commission's new Cyber Security Proceeding (Case 18-M-0376) for determination by the Commission.

To ensure that NextEra's position is not misunderstood, NextEra states that it fully agrees that all customer data, regardless of the source, should be protected. NextEra's point is simply that the Utilities have no right to dictate how NextEra protects its data it collected on its own – in the same way that NextEra has no basis to dictate how the Utilities protect data they collected on their own.

As to the second issue, at the May 31 Meeting, Staff made clear that the intent of the DSA, and this process generally, is to protect the Utilities' systems from infiltration and cyber-attacks. There appears to be a gap between how the ESCOs are accessing the Utilities' systems and what the Utilities believe is occurring. This is evidenced by the broad requirement for cybersecurity insurance, where the risk is simply stated as requiring coverage for an "incident." This term is overly vague, making it very difficult, if not impossible, to secure appropriate insurance coverage. If the situation was reversed and the ESCOs were making this demand, NextEra has no doubt that the Utilities would object to this vague term.

With respect to the third issue, the DSA neglects to include limitations on potential damages, which is inequitable. Liability is not limitless. In the same vein, there also must be a clear linkage between the cause and effect of a data security incident (when properly defined) as ESCO liability should not be unbounded (especially if an "incident" has no discernible negative consequences). Having a mechanism in place at the outset that identifies the cause of an incident and how that incident is dealt with from a liability perspective is vital. Not having an objective process that addresses these issues will lead to significant litigation if an "incident" occurs – the DSA should avoid such an outcome, not create it. These are issues that merit further development and discussion in the Commission's Cyber Security Proceeding.

Strikingly, the concept of mutuality is absent from the DSA. Similar to the Utilities' desire to protect their systems and data, NextEra has a vested interest in protecting its systems and its own customer data. For example, the Utilities have data related to NextEra's business relationships with each customer, pricing, and competitive information that if disclosed would be harmful to its business. Revisions must be made to the DSA that incorporate mutual data protections and processes. A biased and unbalanced DSA is unfair and inequitable, and it is arguably inconsistent with Section 65(3) of the Public Service Law.[5]

[5] The lack of mutual requirements in the DSA arguably gives an undue and unreasonable preference to a utility with respect to its and an ESCO's treatment of data for the same customer.

As to the last concern listed above, the Commission confirmed in the Instituting Order that the proposed DSA is the same document approved in the Community Choice Aggregation ("CCA") Order regarding data security.[6] NextEra submits that there are material differences in how a CCA operates within a municipality and how an ESCO operates in the broader retail market. For example, the method for receiving customer data is quite different. The notion that the DSA approved for CCA is directly transferrable to the retail marketplace is misplaced – in the former, there is essentially no competition for customers and the commodity provider is not subject to the same risks of customer migration as ESCOs are. This is akin to why the Commission has adopted two different UBPs to govern ESCOs and Distributed Energy Resource providers – because the industries operate differently.

Importantly, the ESCO industry was not put on notice that the CCA agreement would be applied to the retail marketplace. Accordingly, NextEra did not participate in CCA proceeding or offer input on the development of the DSA for CCA purposes. ESCOs should not now be penalized for failing to participate in a proceeding that had no stated or implied relevance to them. Indeed, due process has two requirements – notice and an opportunity to be heard. The failure to provide notice violates the ESCOs' due process rights, and the potential for them to be deprived of the ability to conduct their businesses invokes a right for which process was due.

IV. Self-Attestation

As discussed above, NextEra opposes the procedure proposed for implementing data security measures for ESCOs, particularly the premature requirement to execute the Self-Attestation. Indeed, the Self-Attestation appears to be a backdoor way to have ESCOs agree to many of the terms included in the DSA, outside of the DSA. The provisions of the Self-Attestation are overly broad and vague and fail to provide ESCOs with any guidance regarding whether the methods being used are sufficient. Such lack of information makes it difficult for any ESCO to reasonably agree to such terms. Moreover, it is not appropriate for the Utilities to have full and unfettered discretion to terminate ESCOs' EDI transactions. While it is understood that the intent of the Utilities was to be less restrictive so as not to interfere with ESCO business practices, the Self-Attestation goes too far.

Furthermore, similar to the DSA, the Self-Attestation also fails to provide for mutual acknowledgement of security controls by the Utilities. It is not readily known to the ESCOs what security protocols the Utilities have in place to protect customer data and how access to data is controlled. The Utilities also should be required to attest to these requirements.

---

[6] Instituting Order at 3. *See* Case 16-M-0015, Petition of Municipal Electric and Gas Alliance, Inc. to Create a Community Choice Aggregation Pilot Program, Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications (issued October 19, 2017).

V. Conclusion

NextEra respectfully urges the Commission's involvement in this matter. NextEra continues to have significant concerns regarding the procedure and process being employed by the Utilities and believes that they are overreaching into the Commission's domain as regulator. While there is a need for data security requirements to protect customers, the need is equally applicable to the Utilities and ESCOs. Accordingly, the DSA needs to be fair and balanced and provide equal rights, responsibilities, and obligations for both parties. NextEra fully supports increasing security measures for customers, but these issues are technical and require proper consideration, not rushed or arbitrary and ill-conceived one-sided agreements. Further collaborative discussions – on an expedited basis – with the ESCO industry and other interested stakeholders are needed to determine the most appropriate and workable path forward.

Respectfully submitted,

COUCH WHITE, LLP

Amanda De Vito Trinsey

Amanda De Vito Trinsey
Counsel for NextEra Energy Services New York, LLC

Attachment
cc: Active Parties (via email w/att.)
LuAnn Scherer (via email w/att.)
Francis Dwyer, Esq. (via email w/att.)
Mary Krayeske, Esq. (via email w/att.)
Jeremy Euto, Esq. (via email w/att.)
Paul Colbert, Esq. (via email w/att.)
Amy Davis, Esq. (via email w/att.)
Michael Novak (via email w/att.)

DATA SECURITY ADDENDUM

This Data Security Addendum ("Addendum") to the Retail Supplier Operating Agreement (Electric or Gas) effective _____, is made and entered into this _____ day of _____ , 20___ by and between New York State Electric & Gas Corporation, a New York corporation with offices at James A Carrigg Center, 18 Link Dr. P.O. Box 5224 Binghamton NY 13902 ("Utility") and _____, an Energy Services Company ("ESCO") or Direct Customer ("DC") with offices at _____; and together with Utility the ("Parties" and each, individually, a "Party"). This Addendum is incorporated by reference into the Retail Supplier Operating Agreement between the Parties.

RECITALS

WHEREAS, ESCO/DC 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 ESCO/DC aggregated customer information; and

~~WHEREAS, ESCO/DC has obtained consent from all customers from whom the ESCO/DC intends to obtain information from Utility; and~~

Commented [SC1]: Merged into section 4 to avoid duplication.

WHEREAS, Utility and ESCO/DC also desire to enter into this Addendum to establish, among other things, the full scope of ESCO/DC's obligations of confidentiality with respect to the Confidential Utility 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 Utility Information" means, (A) collectively, aggregated and customer-specific information that Utility is~~:~~ ~~(A)~~ required by the Commission to provide to ESCO/DC and (B) any other ~~Utility-specific, aggregated,~~ Personal Data, Sensitive Data~~, or Utility Data,~~ or customer-specific data provided to ESCO/DC by Utility; provided that ~~,~~Confidential Utility Information shall not include: (a) information which is or becomes publicly available other than as a result of a violation of this Agreement or other similar confidentiality agreement; (b) information which is or becomes available on a non-confidential basis from a source which is not prohibited from disclosing such information pursuant to a legal, contractual or fiduciary obligation; (c) information which the ESCO/DC can establish was legally in its possession prior to disclosure by the Utility; or (d) information which the ESCO/DC can establish was developed by or for ESCO/DC independently of the Utility's Confidential Utility Information.

b. "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 ESCO/DC or its Representative's Processing of

Confidential Utility Information; and (B) ~~the Utility's internal requirements and procedures relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESCO/DC or its Representative's Processing of Confidential Utility Information; and~~ (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved Uniform Business Practices ("UBPs").

c. “Data Security Incident” means a situation when ESCO/DC reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Utility Information; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Confidential Utility Information; or (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information, in each case, to the extent such event set forth in subsection (A), (B), or (C) results from a ~~or (D) any~~ breach by ESCO/DC of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by ESCO/DC or any current or former Representatives.

d. “Destroy” means (A) shredding; (B) permanently erasing and deleting; (C) degaussing; or (D) otherwise modifying Confidential Utility Information in paper, electronic, or other means so as to make it unreadable, unreconstructible, and indecipherable. All Confidential Utility Information as may be specifically requested by Utility must be disposed of in a manner described in (A) through (D) herein.

e. “ESCO/DC” shall have the meaning set forth in the Recitals.

f. “Personal Data” means any information that can be used to identify, locate, or contact an individual, including an employee, customer, or potential customer of Utility, including, without limitation: (A) first and last name; (B) home or other physical address; (C) telephone number; (D) email address or online identifier associated with an individual when combined with a password or security question and answer; (E) “Sensitive Data” as defined below; (F) ~~ZIP codes; (G)~~ employment, financial, or health information; or (G~~H~~) any other information relating to an individual, including cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

g. “PSC” or “Commission” shall have the meaning attributed to it in the Recitals.

h. “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 Personal Data 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.

i. “Sensitive Data” is that subset of Personal Data that is identified in applicable law as being protected personal information, including Social Security number, passport number, driver’s license number, Utility customer account number when combined with a security code, access code or password, Municipal Identification (NYCID) when combined with an account number or security code, access code or password, or similar identifier when combined with an account number or security code, access code or password.

j. “Third-Party Representatives” or “Representatives” means those agents of ESCO/DC that are contractors or subcontractors who have access to Confidential Utility Information as part of their performance of services for ESCO/DC.

k. "Utility Data" means customer data held by Utility, whether produced in the normal course of business or at the request of ESCO/DC or an ESCO/DC and whether or not it is provided to ESCO/DC.

2. **Scope of the Addendum.** This Addendum shall govern and apply to all Confidential Utility Information disclosed to ESCO/DC or to which ESCO/DC is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by ESCO/DC (or it its Representatives). All Confidential Utility Information, in whatever form, media, or medium provided or held, and all extracts, compilations, studies, or other documents based on, derived from, or containing Confidential Utility Information, all data electronically exchanged between the Parties, and all correspondence between or among the Parties or their respective Representatives pertaining to the same shall constitute Confidential Utility Information hereunder. No financial information will be provided pursuant to this Addendum. If any financial information is inadvertently sent to ESCO/DC, ESCO/DC will immediately notify the Utility and Destroy any such information in the appropriate manner.

3. **ESCO/DC Compliance with all Applicable Commission Uniform Business Practices.**

_____ESCO/DC is an Energy Services Company ("ESCO/DC") and expressly agrees to comply with the Commission's ESCO/DC Uniform Business Practices ("UBPs"), as they may be amended from time to time.

_____ESCO/DC is a Distributed Energy Resource Supplier ("DERS") and expressly agrees to comply with the Commission's DERS UBPs, as they may be amended from time to time.

_____ESCO/DC is a vendor, agent or other entity providing services to an ESCO/DC or DER.

4. **Customer Consent.** ESCO/DC warrants that it will abide by all laws and regulations concerning the obtaining and storage of customer consents for receiving Confidential Utility Information~~has obtained informed consent from all customers about whom ESCO/DC requests data and that it will retain such consent for a period of at least two years. ESCO/DC agrees to provide proof of customer consent at the request of Utility and Utility reserves its right to audit ESCO/DC for compliance with consent requirements herein. ESCO/DC agrees that upon a customer revocation of consent, ESCO/DC warrants that it will no longer access said customer's information and that it will Destroy any of said customer's information in its or its Representative's possession.~~

5. **Provision of Information.** Utility agrees to provide to ESCO/DC or its Representatives, certain Confidential Utility Information, as requested, provided that (A) ESCO/DC and its Representatives are in compliance with the terms of this Addendum; (B) if required by Utility, ESCO/DC has provided and has caused its Third Party Representatives to provide the executed Self-Attestation form ~~, to~~

~~the satisfaction of Utility any Vendor Product/Service Security Assessments,~~ attached hereto as Exhibit A~~ or such other risk assessment forms as Utility may require from time to time~~ ("Assessment")~~ and ESCO/DC will comply with the Utility Assessment~~

~~requirements~~; and (C) ESCO/DC (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as detailed in the Assessment reasonably acceptable to Utility to protect Confidential Utility Information~~; and (D) ESCO/DC complies and shall cause its Third-Party Representatives to comply with Utility's data protection programs~~. Provided the foregoing prerequisites have been satisfied, ESCO/DC shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to ESCO/DC. Unless otherwise agreed or established by law, ~~Data and/or~~ Confidential Utility Information will at all times remain the sole property of the Party collecting the data and/or Confidential Information. Nothing in this Addendum~~Rider~~ 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.

6. Confidentiality. ESCO/DC shall: (A) hold all Confidential Utility Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) except as otherwise permitted by this Addendum, not disclose Confidential Utility Information to any other person or entity (including but not limited to Third Party Representatives, affiliates, or members of ESCO/DC); (C) not Process Confidential Utility Information outside of the United States; (D) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Addendum; (E) limit reproduction of Confidential Utility Information; (F) store Confidential Utility Information in a secure fashion at a secure location in the United States that is not accessible to any person or entity not authorized to receive the Confidential Utility Information under the provisions hereof; (G) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as ESCO/DC 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 (H) to the extent required by the Utility, each Third Party Representative~~person~~ with a need to know the Confidential Information shall sign the Third-Party Representative Addendum set forth as Exhibit B to this Addendum. At all times, Utility shall have the right to request further assurances that the foregoing restrictions and protections concerning Confidential Utility Information are being observed and ESCO/DC shall be obligated to promptly provide Utility with the requested assurances.

7. Exceptions Allowing ESCO/DC to Disclose Confidential Utility Information.

a. **Disclosure to Representatives**. Notwithstanding the provisions of Section 6 herein, ESCO/DC may disclose Confidential Utility Information to its Third Party Representatives who have a legitimate need to know or use such Confidential Utility Information for the sole and limited purposes of providing Services, provided that each such Third Party Representative first (A) is advised by ESCO/DC of the sensitive and confidential nature of such Confidential Utility Information; (B) agrees to comply with the confidentiality provisions of

this Addendum, 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 Addendum as though such Third Party Representatives were ESCO/DC; and (C) signs the Third Party Representative Addendum. All such written Addendums with Third Party Representatives shall include direct liability for the Third Party Representatives towards Utility for breach thereof by the Third Party Representatives, and a copy of such Addendum and each Third Party Representative Addendum and ESCO/DC Addendum shall be made available to Utility upon request. Notwithstanding the foregoing, ESCO/DC shall be liable to Utility for any act or omission of a Third Party Representative, including without limitation, Third Party Representatives that would constitute a breach of this Addendum if committed by ESCO/DC.

b. **Disclosure if Legally Compelled**. Notwithstanding anything herein, in the event that ESCO/DC 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 Utility 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), ESCO/DC shall, except to the extent prohibited by law, within 72~~24~~ hours notify Utility or such longer time as may be commercially practicable given the circumstances, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, Utility shall have the right to consult with ESCO/DC 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 Utility Information that must be disclosed. Utility shall also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Utility Information that must be disclosed. In any event, ESCO/DC and its Third Party Representatives shall disclose only such Confidential Utility 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 Utility) and ESCO/DC and its Third Party Representatives shall use ~~all~~ reasonable efforts to ensure that all Confidential Utility Information that is so disclosed will be accorded confidential treatment.

8. **Return/Destruction of Information**. R E S E R V E D . ~~Within ten (10) days after Utility's written demand, ESCO/DC 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) 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 ESCO/DC's or its Third Party Representatives' possession, including destroying Confidential Utility Information from all systems, records, archives, and backups of ESCO/DC and its Third Party Representatives,~~

~~and all~~

~~subsequent access, use, and Processing of the Confidential Utility Information by ESCO/DC and its Third Party Representatives shall cease. Notwithstanding the foregoing, ESCO/DC 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 ESCO/DC and its Third Party Representatives shall (1) not have experienced a Data Security Incident, (2) not permit 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 Addendum. ESCO/DC shall, upon request, certify to Utility that the destruction by ESCO/DC and its Third Party Representatives required by this Section has occurred by (A) having a duly authorized officer of ESCO/DC 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 ESCO/DC from compliance with the other provisions of this Addendum. The obligations under this Section shall survive any expiration of termination of this Addendum.~~

9. **Audit.** Upon reasonable notice to ESCO/DC, ESCO/DC shall, and shall require its Third Party Representatives to permit Utility, its auditors, designated audit representatives, and regulators to audit and inspect, at Utility's sole expense (except as otherwise provided in this Addendum), and no more often than once per year (unless otherwise required by Utility's regulators): (A) the facilities of ESCO/DC and ESCO/DC's Third Party Representatives where Confidential Utility Information is Processed by or on behalf of ESCO/DC; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESCO/DC'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 and inspection rights shall be for the sole purpose ~~, at a minimum, for the purpose~~ of verifying ESCO/DC's compliance with this Addendum, including all applicable Data Protection Requirements. Notwithstanding anything herein, in the event of a Data Security Incident, ESCO/DC shall and shall cause its Third Party Representatives to permit an audit hereunder more frequently than once per year, as may be requested by Utility. ESCO/DC shall promptly~~immediately~~ correct any deficiencies identified by Utility.

10. **Investigation.** Upon notice to ESCO/DC, ESCO/DC 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 ESCO/DC 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 ESCO/DC or its Representatives, in which case such assistance shall be at ESCO/DC's sole expense.

11. **Data Security Incidents.** ESCO/DC is responsible for any and all Data Security Incidents involving Confidential Utility Information that is Processed by, or on

behalf of, ESCO/DC. ESCO/DC shall notify Utility in writing promptly~~immediately~~ (and in any event within twenty-four (24) hours) whenever ESCO/DC, after investigation, ~~-~~reasonably believes that there has been a Data Security Incident. After providing such notice, ESCO/DC will investigate the Data Security Incident, and ~~immediately~~ promptly 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. ESCO/DC further agrees to provide, at ESCO/DC's sole cost, 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 and/or the mitigation of any damage, including any notification required by law ~~or that Utility may determine appropriate~~ to send to individuals impacted or potentially impacted by the Data Security Incident. ~~, and/or the provision of any credit reporting service required by law or that Utility deems appropriate to provide to such individuals. Unless required by law, ESCO/DC shall not notify any individual or any ESCO/DC other than law enforcement of any potential Data Security Incident involving Confidential Utility Information without first consulting with, and obtaining the permission of, Utility. In addition, within 30 days of identifying or being informed of a Data Security Incident, ESCO/DC shall develop and execute a plan, subject to Utility's approval, that reduces the likelihood of a recurrence of such Data Security Incident. ESCO/DC agrees that Utility may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Addendum if a Data Security Incident occurs~~.

12. Cybersecurity Insurance Required. ESCO/DC shall carry and maintain Cybersecurity insurance in an amount of no less than $10,000,000 per incident. ~~and Utility shall be included by endorsement as an additional insured on ESCO/DC's Cybersecurity insurance. ESCO/DC agrees to cause its Third Party Representatives to carry and maintain cybersecurity insurance in the amount shown above.~~

13. No Intellectual Property Rights Granted. Nothing in this Addendum 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 ESCO/DC shall acquire no ownership interest in the Confidential Utility Information (which, as between ESCO/DC and Utility, shall be and remain the proprietary and confidential information of Utility)~~. No rights or obligations other than those expressly stated herein shall be implied from this Addendum.

14. Additional Obligations.

a. ~~ESCO/DC shall not create or maintain data which are derivative of Confidential Utility Information except for the purpose of performing its obligations under this Addendum or as authorized by Utility.~~ Data collected by ESCO/DC from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging

with ESCO/DC or its partners shall not be considered Confidential Utility

Information or a derivative of Confidential Utility Information for the purpose of this Addendum.

b. ESCO/DC 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 ESCO/DC to be applicable to Utility.

c. ESCO/DC shall have in place appropriate and reasonable processes and systems, including an Information Security Program 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 ESCO/DC's internal use, Processing, or other transmission of Confidential Utility Information, whether between or among ESCO/DC's Third Party Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of ESCO/DC, including without limitation Third Party Representatives.

d. ESCO/DC shall safely secure or encrypt all Confidential Utility Information during ~~storage or~~ transmission.

e. ESCO/DC 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 ESCO/DC to the extent such request, complaint or other communication relates to ESCO/DC's Processing of such individual's Confidential Utility Information.

f. ESCO/DC 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 ESCO/DC's accessing or Processing of such Confidential Utility Information.

15. **Payment.** In consideration of Utility's Addendum to provide Confidential Utility Information in accordance with Section 2, ESCO/DC shall pay to Utility applicable fees pursuant to its tariffs.

16. **Specific Performance.** The Parties acknowledge that disclosure or misuse of Confidential Utility Information in violation of this Addendum 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 seek specific performance and/or injunctive relief to enforce compliance with the provisions of this Addendum. Utility's right

to such

relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Addendum, at law or in equity, including monetary damages, the right to terminate this Addendum for breach and the right to suspend the provision or Processing of Confidential Utility Information hereunder. ~~ESCO/DC 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 and hereby authorizes, to the extent lawfully possible, any court of competent jurisdiction to dispense with any requirement for such bond or other security which might otherwise be judicially imposed.~~

17. Indemnification. To the fullest extent permitted by law, ESCO/DC 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) to the extent arising out of~~, relating to, or resulting from, in whole or in part,~~ the breach or non-compliance with this Addendum by ESCO/DC or any of its Third Party Representatives that results in a Data Security Incident.

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 ESCO/DC, to:

ESCO/DC Name:
Name of Contact:
Address:
Phone:
Email:

If to Utility, to:

New York State Electric & Gas Corporation
Name of Contact: Supplier Relations
Address: James A Carrigg Center
18 Link Dr.
P.O. Box 5224
Binghamton NY 13902

Email: supplier_relations@rge.com

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.

19. **Term.** This Addendum shall be effective as of the date first set forth above and shall remain in effect until terminated by Utility upon not less than 10 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 Addendum prior to the effective date of termination; and provided, further, that Utility may terminate this Addendum immediately upon notice to ESCO/DC in the event of a material breach hereof by ESCO/DC or its Third Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 16, and 24 shall be a material breach hereof. Upon the expiration or termination hereof, neither ESCO/DC nor its Third Party Representatives shall have any further right to Process Confidential Utility Information and shall immediately comply with its obligations under Section 8.

20. **Consent to Jurisdiction; Selection of Forum**. ~~ESCO/DC~~Each party irrevocably submits to the jurisdiction of the courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Addendum. ~~ESCO/DC~~Each party agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ~~ESCO/DC~~such party at the address for ~~ESCO/DC~~such party 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. ~~ESCO/DC~~Each party agrees that service of process on it may also be made in any manner permitted by law. ~~ESCO/DC~~Each party consents to the selection of the New York State and United States courts within Dutchess County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Addendum.

21. **Governing Law.** This Addendum 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.

22. **Survival.** The obligations of ~~ESCO/DC~~each party under this Addendum shall continue for so long as ESCO/DC and/or ESCO/DC's Third Party Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all Addendums between ESCO/DC and Utility have expired or been terminated.

23. **Counterparts.** This Addendum 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 Addendum and copies of signatures on this Addendum, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.

24. **Amendments; Waivers.** This Addendum 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 Addendum 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.

25. **Assignment.** This Addendum (and Aggregator's obligations hereunder) may not be assigned by ESCO/DC or Third Party Representatives without the prior written consent of Utility, and any purported assignment without such consent shall be void.

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

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

28. **No Third-Party Beneficiaries.** This Addendum is solely for the benefit of, and shall be binding solely upon, the Parties and their respective agents, successors, and permitted assigns. This Addendum 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 Addendum.

29. **Force Majeure.** No Party shall be liable for any failure to perform its obligations in connection with this Addendum, where such failure results from any act of God 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 Addendum and which such Party is unable to prevent or overcome after the exercise of reasonable diligence.

30. **Relationship of the Parties.** Utility and ESCO/DC 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 Addendum 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.

31. **Construction.** This Addendum shall be construed as to its fair meaning and not strictly for or against any party.

32. **Binding Effect.** No portion of this Addendum 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.

33. **Limitation of Liability.** NOTWITHSTANDING ANYTHING CONTAINED IN THIS AGREEMENT, EACH PARTY'S LIABILITY TO THE OTHER PARTY IN CONNECTION WITH THIS AGREEMENT AND ANY ACTIVITIES UNDERTAKEN IN CONNECTION HEREWITH SHALL BE LIMITED TO DIRECT DAMAGES AND SHALL EXCLUDE ANY OTHER LIABILITY, INCLUDING WITHOUT LIMITATION LIABILITY FOR SPECIAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES IN CONTRACT, TORT, WARRANTY, STRICT LIABILITY OR OTHERWISE. NOTWITHSTANDING ANYTHING CONTAINED IN THIS ADDENDUM TO THE CONTRARY, THE ESCO/DC'S LIABILITY TO THE UTILITY IN CONNECTION WITH THIS ADDENDUM AND ANY ACTIVITIES UNDERTAKEN OR NOT UNDERTAKEN RELATED TO SUCH ADDENDUM WILL NOT EXCEED TEN MILLION DOLLARS ($10,000,000).

34. **Waiver of Trial by Jury.** TO THE EXTENT PERMITTED BY LAW, EACH OF THE PARTIES HERETO HEREBY KNOWINGLY, VOLUNTARILY AND INTENTIONALLY WAIVES THE RIGHT EITHER OF THEM MAY HAVE TO A TRIAL BY JURY IN RESPECT OF ANY LITIGATION BASED HEREON, OR ARISING OUT OF, UNDER OR IN CONNECTION WITH THIS AGREEMENT. THIS PROVISION IS A MATERIAL INDUCEMENT FOR THE PARTIES ENTERING INTO THIS AGREEMENT.

[Signature page follows]

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

New York State Electric and Gas Corporation	_____ ESCO/DC
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

EXHIBIT A

~~**Vendor Product/Service Security Assessments**~~

~~**Data Security Questionnaire**~~

~~1. Is your computer network internal to your organization or do you have it hosted by a cloud / colocation vendor? If so, what vendor do you use?~~
~~2. What technical security measures has the vendor taken to protect its network?~~
   ~~a. Firewall,~~
   ~~b. Intrusion detection / prevention system,~~
   ~~c. Anti-virus / anti-malware,~~
   ~~d. Data loss prevention,~~
   ~~e. Endpoint protection,~~
   ~~f. Network access control,~~
   ~~g. Data encryption,~~
   ~~h. Vulnerability scanning,~~
   ~~i. Identity access management,~~
   ~~j. Password management,~~
   ~~k. Security alerting, audit logging, etc.,~~
   ~~l. Remote access.~~
   ~~m. Other Security Measures.~~
~~3. What procedural security measures has the vendor taken to protect its network?~~
   ~~a. Timely removal of terminated employees,~~
   ~~b. Security awareness training – focus on phishing emails (required by PSC),~~
   ~~c. Security policies & procedures (e.g. computer use policy, incident response plan, disaster recovery plan, security policy, risk management policy, etc.),~~
   ~~d. Incident response procedures,~~
   ~~e. System pre-implementation testing,~~
   ~~f. Change management controls,~~
   ~~g. Physical security controls over computer room,~~
   ~~h. Background checks on IT personnel,~~
   ~~i. Framework (CoBIT, ISO 27001),~~
   ~~j. Employee signed NDA,~~
   ~~k. Data privacy controls, etc.~~
   ~~l. Other procedural security measures.~~
~~4. How is the data transferred? Will it be encrypted in transit?~~

~~5. Where is the data physically located? (in the U.S. or foreign country)~~

~~6. How is the data stored and backed up? Will it be encrypted?~~

~~7. How do you ensure that unauthorized access is prevented?~~

8. Do you allow your employees to save Utility data to a local or removable device or to print Utility data?

9. Upon Utility request, how would you either return or delete Utility data (both electronic and hardcopy for production and backup systems)?

10. Are personnel able to access Utility data from a mobile device? If so, what security measures have you taken to protect the device?

11. Do you have ESCO/DC security assessments / audits performed on your network? (penetration test, vulnerability testing, SSAE 16 SOC 2 audit).

12. Do you have cyber insurance of $10 million?

13. Does the vendor use outsourced third parties to assist in providing the service?

14. Will ESCO/DC or Third Party Representatives use cloud computing software / hardware to provide the service?

EXHIBIT A

Data Security Rider

I. General

(1) This Data Security Rider shall apply to ESCO/DC in the event that ESCO/DC is granted or has access, in any way, to Utility's data and/or Confidential Information.

(2) Definitions:

i. "Cardholder Data" means a User's individual credit or debit card cardholder name, number, expiration date, the Card Security Code/Card Verification Value/Card Validation Code/Card Authentication Value, or Card Identification Number/Card Authentication Value 2/Card Validation Code 2/Card Verification Value 2.

ii. "Confidential Information" has the meaning set forth in this Addendum.

iii. "Customer Information" means a Utility electric or gas delivery Utility or ESCO/DC customer's account number, name, address, zip code, phone number, email address, social security number, bank account number or routing number, credit card information, driver's license number, billing or usage data, enrollment in a low income or similar program, health status, including being on life support, meter Global Positioning System ("GPS") coordinates, or information regarding a customer's personal residence, such as square footage, smart appliances in residence, home network internet protocol address.

iv. "Cyber Event" means (a) any occurrence in an information system or network that has, or may potentially result in, unauthorized access, processing, corruption, modification, transfer or disclosure of data and/or Confidential Information or (b) a violation of an explicit or implemented Company security policy.

v. "Cyber Incident" means (a) the loss or misuse (by any means) of data and/or Confidential Information; (b) the inadvertent, unauthorized and/or unlawful access, processing, corruption, modification, transfer, disclosure, sale or rental of Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity, availability, or privacy of data and or Confidential Information protected by this Addendum.

vi. "Data" means all: (i) drawings, plans, maps, diagrams, charts, calculations, sketches, illustrations, designs and design layouts (collectively the "Drawings"), (ii) written technical specifications, design criteria, engineering data and all other information and data relating to the exchange of information between the Parties including Confidential Information, (iii) computer programs, software and source codes, (iv) operating and maintenance manuals with respect to the exchange of information, and (v) any other written or otherwise recorded information relating to the Addendum and its Exhibits ; which are either annexed to or referred to in the Addendum or this Data

Security Rider ("Rider") or required to be supplied by ESCO/DC pursuant to the terms of the Addendum or its Exhibits or which Utility may reasonably require in connection with this Addendum.

vii. "Personal Identifiable Information" ("PII") is defined as customer account number, name, address, phone number, electric or gas usage, billing amounts, social security numbers, driver's license number, credit card number, debit card number, or banking information.

viii. "Third Party Representative" means any individual, firm or corporation engaged directly or indirectly by ESCO/DC in performance of any obligation pursuant to this Addendum, including any individual, firm or corporation that is an affiliate, agent, or assigned of ESCO/DC.

ix. "Users" means a Utility electric or gas delivery customer.

II. Privacy and Data Security

(1) Data and/or Confidential Information will at all times remain the sole property of the Party collecting the data and/or Confidential Information. Nothing in this Rider 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.

(2) ESCO/DC shall provide annual security awareness training to any individual who has access to Utility's data or who transmits data to Utility ("Access Individuals"). Upon Utility's request, ESCO/DC shall promptly provide to Utility evidence that all Access Individuals have received such training.

(3) ESCO/DC must provide 20 business days prior written notice to Utility if a new Third Party Representative will be engaged by ESCO/DC to support the data exchange with Utility. ESCO/DC will assist Utility in providing information, in form and substance sufficient to Utility, regarding the state of the internal control environment of the Third Party Representative to enable Utility to perform any security assessment that Utility deems necessary. Utility reserves the right to reject any proposed Third Party Representative if the Third Party Representative's internal control environment does not meet Utility's requirements.

(4) ESCO/DC shall ensure that any Third Party Representative is bound by terms and obligations at least as stringent as those set forth in this Addendum and Data Security Rider. Utility reserves the right to audit such terms and obligations and to determine, in its sole discretion, whether or not the obligations and terms are sufficient.

(5) At any and all times during which ESCO/DC or Third Party Representative is engaged in data exchange with Utility, ESCO/DC and its Third Party Representative(s) will:

i. Have appropriate and reasonable security controls and/or measures in place to protect and safeguard the data exchange with Utility from disclosure or unauthorized access and/or use. ESCO/DC and its Third Party Representative(s) shall secure its computer systems, network, and devices

using a defense-in-depth approach, compliant with industry recognized best practices or frameworks (e.g., NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls, etc.).

ii. Have appropriate and reasonable privacy controls and/or measures to protect the data exchange with Utility and Utility's data according to industry recognized best practices or frameworks (e.g., DOE Data Guard Energy Data Privacy Program, AICPA Generally Accepted Privacy Principles, NISTIR 8062, ISO 29100, etc.).

iii. Comply with all applicable privacy and security laws, regulations, of New York State Public Service Commission Orders to which ESCO/DC or Utility is subject and not, by act or omission, place Utility in violation of any privacy or security law, regulation or order known by ESCO/DC to be applicable to Utility.

iv. Promptly notify Utility of any material change(s) to the ESCO/DC's security policies, procedures, controls or measures.

v. Safely secure or encrypt data during storage or transmission.

vi. Store data only within the boundaries of the United States.

vii. Except as may be necessary in connection with the data exchange, not store data on removable devices or media.

viii. Not back up data to the cloud without Utility's prior written approval.

(6) If ESCO/DC uses a service provider or co-location data center, ESCO/DC will do so only if in compliance with the complementary user entity controls stated in the service provider's or co-location's SSAE 16 audit report.

(7) If the data exchange includes the use of ESCO/DC's hosted site(s), a privacy statement shall be present on the site that, at a minimum, includes the same language as in Utility's privacy statement located at: http://www.nyseg.com/legaldisclaimer.html.

(8) To the extent that ESCO/DC or Third Party Representative processes credit card transactions as part of providing services and includes that data as part of the data exchange, the following requirements shall apply with respect to the Cardholder Data:

i. ESCO/DC and its Third Party Representative(s) represent that it is presently in compliance, and will remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS"), and all updates to PCS DSS, developed and published jointly by American Express, Discover, MasterCard and Visa ("Payment Card Brands") for protecting Cardholder Data.

ii. ESCO/DC and its Third Party Representative(s) acknowledges that Cardholder Data is owned exclusively by the data transmitter, credit card issuers, the relevant Payment Card Brand, and entities licensed to process credit and debit card transactions on behalf of Utility, and further acknowledges that such Cardholder Data may be used solely to assist the foregoing parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for other uses specifically required by law, the operating regulations of the Payment Card Brands, or this Addendum, including this Data Security Rider.

iii. ESCO/DC and its Third party Representative(s) agrees that, in the event of a Cyber Incident arising out of or relating to ESCO/DC or Third Party Representative's premises or equipment contained thereon, ESCO/DC and Third Party Representative(s) shall provide full cooperation and access to its premises, books, logs and records by a designee of the Payment Card Brands to the extent necessary to perform a thorough security review and to validate ESCO/DC's or Third Party Representative's compliance with the PCI DSS.

(9) If Utility wishes to discontinue the use of a hosted system and retrieve all Utility Data, ESCO/DC and its Third Party Representative(s) shall ensure administrative interfaces and open APIs exist that provide access to all Utility Data. With sufficient additional technical services resources and sufficient available bandwidth, all Utility Data will be retrieved within 15 business days by Utility and Utility will authorize the ESCO/DC and Third Party Representative to delete the Data from within the hosted system in a manner consistent with the Addendum.

III. **System Development**

(1) To the extent that ESCO/DC exchanges data with Utility, ESCO/DC and its Third Party Representative(s) shall agree to apply the following requirements:

i. Establish policies and procedures that ensure the application system has been designed, built and implemented in a secure manner according to industry recognized best practices or frameworks (e.g., Build Security in Maturity Model (BSIMM) benchmarks, Open Group ACS Trusted Technology Provider framework, NIST, OWASP, etc.).

ii. Establish policies and procedures that ensure data security has been designed, built, and implemented into the application system according to industry recognized best practices or frameworks (e.g.,CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS, etc.).

iii. Establish policies and procedures that ensure the application system has been properly tested, including the development of a security test plan that defines an approach for testing or otherwise establishing that each of the security requirements has been met.

iv. Perform vulnerability assessment and penetration test on the application system to identify any security issues prior to the application system being placed into production. ESCO/DC or its Third Party Representative(s) verify that appropriate and reasonable action will be taken to mitigate any security issues identified prior to the system being placed into production.

v. Upon Utility's request, ESCO/DC and each Third Party Representative shall promptly provide the results of any vulnerability assessment and penetration test.

vi. Establish policies and procedures that ensure the application system has a proper change management and patch management process that includes applying, testing, and validating the appropriate changes / patches before being placed in the production system.

vii. Upon Utility's request, ESCO/DC and each Third Party Representative shall promptly provide a self-certification letter to Utility verifying that the application system meets the security requirements stated in the Data Security Rider, that all security activities have been performed, and all identified security issues have been documented and resolved.

(2) ESCO/DC warrants that the application system contains no virus, Trojan, worm, undocumented shutdown mechanism or other code or feature which is intended, or is known by ESCO/DC as likely, to disable, damage, destroy, deny access to or degrade the performance of the application system, or Confidential Information, Data or other information technology resource. ESCO/DC warrants that the application system contains no backdoors or other feature that is intended to allow ESCO/DC or someone else to gain unauthorized or surreptitious access to the application system or Data or other information technology resources. ESCO/DC agrees to indemnify and hold Utility harmless from any claims, damages, causes of action, costs and expenses arising out of or related to any breach of the warranty set forth in this Section.

IV. Incident Reporting

(1) It shall be presumed that the consequences of a virus, worm, Trojan, hacker intrusion or similar network security breach is not beyond the control of the ESCP or its Third Party Representative(s).

(2) ESCO/DC shall remain responsible for any Cyber Event or Cyber Incident in relation to its or its Third Party Representatives' obligation set forth in the Addendum and Data Security Rider.

(3) ESCO/DC and their Third Party Representative(s) shall notify Utility of a cyber-incident based on the Notification Table. Upon Utility's request, ESCO/DC shall utilize and pay the cost for a computer forensic expert to investigate the incident that is either provided by ESCO/DC or Utility.

Classification	Description	Notification By
Low	• System unavailable affecting 5% of Users.	Within 24 hours upon identification
Medium	• System unavailable affecting 10% of Users. • Cyber Event as defined in the Data Security Rider.	Within 8 hours upon identification
High	• System unavailable affecting 15% of Users. • Cyber Incident as defined in the Data Security Rider. • User request, complaint or other communication regarding potential misuse or unauthorized access to User's customer information.	Immediately upon identification

(4) ESCO/DC and its Third Party Representative(s) shall establish policies and procedures to properly investigate a Cyber Event or Cyber Incident and be willing to work with Utility's forensic examiner.

(5) Notification will be made to the main contact at Utility and to supplier_relations@rge.com.

V. Right to Audit

(1) Upon Utility's request, ESCO/DC shall provide reasonable evidence that the controls of ESCO/DC and its Third Party Representative(s) include the proper security controls in place to protect Utility's data and to ensure that ESCO/DC's Third party Representatives' information systems related to the data exchange are operating effectively to ensure availability. The evidence may include, as determined by Utility, ESCO/DC audit reports, such as the AICPA's SSAE 16 SOC 1 and SOC 2 (all 5 of the trust principles) reports or a penetration test report, or a certification letter from a ESCO/DC verifying that that ESCO/DC and its Third party Representative(s) are in compliance, such as an ISO 27001 or PCI DSS certification letter.

Utility may also, at its discretion, perform a security controls audit or penetration testing of ESCO/DC upon notice to ESCO/DC of not less than 30 business days. ESCO/DC shall include in each of its Contracts with each of its Third Party Representative(s) a right for Utility to audit their services. ESCO/DC is responsible for addressing any user entity control requirements and any control deficiencies or findings that are noted in these audit reports.

EXHIBIT B

THIRD-PARTY REPRESENTATIVE ADDENDUM

I, _____, have read the Addendum between _____, ("Company") and New York State Electric & Gas Corporation, ("Utility") dated _____ ___, 20___(the "Addendum") 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 ESCO/DC pursuant to the Addendum.

_____ _____

Signature Date

EXHIBIT A

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

NextEra objects to this Self-Attestation document in its entirety, including, but not limited to, for the following reasons:

1. NextEra is deemed eligible to sell retail electricity in the State of New York and there is no law or regulation that requires it to divulge sensitive information security practices to third parties as a condition to operate in New York's retail marketplace.

2. Divulging sensitive information security practices to third parties is not best practice and actually increases the risk to ESCO's systems and the ESCO consumer information stored on those systems.

3. The Joint Utilities have not identified which potentially harmful practices they are trying to solve for, and thus, the information below is a "fishing expedition" which puts consumer information directly at risk.

4. The content of this "attestation" is overly broad, subjective and vague. There is no way to fully understand the assumptions made by the Joint Utilities and what qualifies as "non-compliance". ESCO should not be set up to fail an attestation because they could not guess what the Joint Utilities' were intending.

5. The attestation is not mutual and fails to provide the same confirmation of security controls to protect ESCO customer information.

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 (as defined previously 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).

The Requirements are as follows (check all that apply to Third Party's computing environment):

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

_____ A risk-based Information Security Program exists to manage policy requirements.

An Incident Response Procedure is implemented that includes notification within 24 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 an at-least monthly 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, workstations, and mobile devices 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 encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.

_____ All forms of mobile and removable storage media, including, but not limited to, laptop PCs, mobile phones, backup storage media, external hard drives, and USB drives must be encrypted.

_____ All Confidential Utility Information is stored in the United States only, including, but not limited to, cloud storage environments and data management services.

_____ 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 other security controls audit report.~~

~~Upon reasonable notice to Third Party, Third Party shall permit Utility, its auditors, designated audit representatives, and regulators to audit and inspect facilities, including computerized and paper systems, where Confidential Utility Information is processed or stored, and relevant security practices, procedures, records, and technical controls. Such audit and inspection rights shall be, at a minimum, for the purpose of verifying Third Party's compliance with this Attestation. If Third Party provides an up-to-date SOC II Type 2 Audit Report, the respective Third Party will not be chosen for audit for one year after submission of the Report. If Third Party provides an alternative security controls audit report, it is at the JU's discretion, individually as a Utility or collectively, in whole or part, of if the respective Third Party is absolved of potential audit for one year.~~

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

Signature: _____

Name: _____

Title: _____

Date: _____