Phillips Lytle LLP

June 22, 2018

By Electronic Filing

Utility Representatives
Regarding Data Security Agreements

Dear Representative:

On behalf of Family Energy Inc. ("Family Energy") we respectfully submit these comments on the Data Security Agreements ("DSAs" or singularly, "DSA") provided by the following utilities: National Grid/Niagara Mohawk ("NIMO")/KeySpan Gas East Company ("KEDLI")/Brooklyn Union Gas Company ("KEDNY"); Central Hudson; Consolidated Edison Company of New York ("ConEd")/Orange & Rockland ("O&R"); Rochester Gas & Electric ("RG&E")/New York State Electric & Gas ("NYSEG") (collectively, "DSA Utilities").

Attached hereto please find redlines of the various forms of DSA provided by Central Hudson, Con Ed/Orange & Rockland; RG&E/NYSEG (using the RG&E form), and National Grid (using the KEDNY form).

Family Energy is eager to cooperate, but objects to the manner in which this process is being undertaken as unnecessarily rushed, disorganized, wasteful and significantly unfair. Moreover, the DSA's are overly broad and cause significant, costly business disruption and harm that is not proportional to the sensitivity (if any) of the data at issue.

The form of DSA, taken from the Community Choice Aggregation Program, is simply not well suited to the ESCO-Utility relationship. Discussion at the May 31, 2018 data security meeting made clear that EDI transactions are unlikely to cause risks warranting DSA-type measures. Nor should access to Utility-provided web-platforms create risks that are materially increased by ESCO usage. No technical or substantive response to these facts has been provided; only threats of discontinuance.

ATTORNEYS AT LAW

THOMAS F. PUCHNER, PARTNER DIRECT **518 618 1214** TPUCHNER@PHILLIPSLYTLE.COM

OMNI PLAZA 30 SOUTH PEARL STREET ALBANY, NY 12207-3425 PHONE **518 472 1224** FAX **518 472 1227**

NEW YORK: ALBANY, BUFFALO, CHAUTAUQUA, GARDEN CITY, NEW YORK, ROCHESTER | **WASHINGTON, DC** | **CANADA:** WATERLOO REGION | PHILLIPSLYTLE.COM

Many aspects of the process simply do not make sense. For example, the DSA forms require the same level of security and insurance be flowed down to subcontractors and vendors of ESCOs. Some adjustment should be made based on the level of interaction with allegedly Confidential Utility Data and Utility systems, and that the Utilities themselves will also agree to these requirements. To the extent there is any risk, the level posed by an EDI vendor processing billing and enrollment transactions is significantly different than a marketing vendor or broker accessing one-at-a-time account information and usage history.

The forms appear to require ESCO vendors to both sign the DSA independently (as "vendor, agent or other entity providing services to an ESCO or DER," in Section 3), and execute a Third Party Representative Agreement for each ESCO. National Grid omitted the Third Party Representative form completely from some of the agreements circulated. ConEd never provided it at all. Upon multiple inquiries, ConEd advised that it was not requiring that form. As a result, the ConEd DSA contains internal inconsistencies that do not make sense in the current form.

The DSAs require intrusive audits of systems and facilities by utility auditors or audit representatives. No provision is made for securing information obtained by auditors about ESCO and vendor systems, facilities and security. How will this information be protected? What assurances will be in place?

Lastly, there have been unreasonable timelines imposed throughout this process. Initially, DPS Staff demanded same day information regarding use of ESG/Latitude. Shortly afterwards, NIMO circulated a DSA form that it required ESCOs to return in just seven days—under threat of termination of service (again, circulated without all of the attachments). Later, other varying utility deadlines were provided for other forms of DSA. Currently, ESCOs are asked to participate in a DSA comment process, but demanded to sign a Self-Attestation of Information Security Controls ("Attestation") that should, in fairness, be the subject of comment and discussion as part of the DSAs. Certain requirements (such as audit policies) and critical defined terms are shared between the DSA and Attestation. ESCOs do not know what they are ultimately

attesting to until the terms of the DSA and Attestation are finalized through the comment/revision process. Yet, notwithstanding all of the problems with this process and the proposed DSAs, the unilateral threat of termination remains.

At the time that the Public Service Commission ("PSC") began the retail marketplace, it permitted utilities developing retail access programs to utilize "operating agreements," "handbooks" and similar documents to facilitate business relations with then-new ESCOs. Because these key aspects of the business relationship were not being tariffed, the PSC expressly reserved authority to resolve disputes regarding the terms of such business relationships. 98-E-0952 - *Matter of Competitive Opportunities Regarding Electric Service*, Statement of Regulatory Policies Regarding Operating Agreements (issued Mar. 10, 1998), at 8 (stating that "we shall reserve authority over the [operating] agreements, and, if appropriate, resolve disputes that the parties can not reconcile themselves"); *see also* 96-E-0909 - *Matter of Central Hudson Gas & Electric Corporation's Plans for Electric/Rate Restructuring Pursuant to Opinion 96-12*, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 21-22 & n.1 (citing to Statement of Regulatory Policy, and referencing previously reserved authority to resolve disputes for both operating agreements and handbooks). At the time, the agency expressly directed that operating agreements may not contain fees that are not provided in the relevant tariff in order to avoid unilateral imposition of unreasonable or burdensome fees. *Id.* at 22-23; *see also* Case 96-E-0891 - *Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing*, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 30, 1998), at 25. In this case, the DSAs are unilaterally requiring an exorbitant amount of insurance that bears no rational relation to the risks created by ESCO-Utility interactions. A $10 million insurance policy requirement will create a burden that cannot be borne without impacting customer rates broadly across the industry.

Family Energy's participation in the comment process shall in no way be considered a waiver of rights. Family Energy respectfully reserves all rights, including further and amended filings regarding the DSA and Attestation forms.

Notwithstanding the foregoing, Family Energy looks forward to working with the DSA Utilities to establish policies that are fair and workable.

Respectfully submitted,

Phillips Lytle LLP

By *Thomas F. Puchner*

Thomas F. Puchner
TFP

Comments to Data Security Addendums

TABLE OF CONTENTS

DATA SECURITY AGREEMENT

THIS DATA SECURITY AGREEMENT, including Exhibits attached hereto and made a part hereof (this "Agreement") which are incorporated by reference herein, is made as of this _____ day of _____ , 2018 (the "Effective Date") by and between Consolidated Edison Company of New York, Inc. and Orange and Rockland Utilities, Inc., a New York corporation with offices at 4 Irving Place, New York, NY 10003 ("Utility") and_____ _____ , a third party ("Third Party") with offices at _____ ; and together with Utility the ("Parties" and each, individually, a "Party").

RECITALS

WHEREAS, Third Party 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 Third Party aggregated customer information; and

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

WHERAS, Utility and Third Party also desire to enter into this Agreement to establish, among other things, the full scope of Third Party'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, collectively, aggregated and customer-specific information that Utility is: (A) required by the Commission to provide to Third Party and (B) any other Utility-specific, aggregated, Personal Data, Sensitive Data, or Utility Data, or customer-specific data provided to Third Party by Utility. Confidential Utility Information shall not include any information of Third Party which: (A) was in the public domain at the time of disclosure by Utility to Third Party; (B) became part of the public domain after disclosure by Utility to Third Party through no fault of Third Party; (C) was acquired by Third Party independently after disclosure by Utility to Third Party, from a third party without breach of agreement or violation of law; or (D) was in Third Party's possession prior to the time of disclosure by Utility to Third Party. For avoidance of doubt, data collected by Third Party from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with Third Party or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Agreement.

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 Third Party or its Representative's Processing of Confidential Utility

Information; (B) the Utility's internal requirements and procedures that are provided by Utility to Third Party relating to the protection of information that identifies or can be used to identify an individual that apply with respect to Third Party 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 Third Party 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,

0

Comment [pl1]: An inadvertent corruption of data could be a normal business event fixed through routine backup procedures. This should not be deemed a Data Security Incident.

modification, transfer, sale or rental of Confidential Utility Information; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by Third Party or any current or former Representatives. Good faith acquisition of Confidential Utility Information by an employee or agent of Third Party for the purposes of the business is not a Data Security Incident, provided that the Confidential Utility Information is not misused or subject to unauthorized disclosure.

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, except as otherwise required by law, including but not limited to record retention requirements and litigation holds.

e. "Third Party" 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; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial, or health information; or (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, including Social Security number, passport number, driver's license number, Utility customer account number, Municipal Identification (NYCID), or similar identifier.

j. "Third-Party Representatives" or "Representatives" means those agents of Third Party that are Electronic Data Interchange vendors, contractors or subcontractors.

k. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of Third Party or a third party and whether or not it is provided to Third Party.

2. Scope of the Agreement. This Agreement shall govern and apply as of the Effective

Comment [pl2]: Same comment as above

Comment [pl3]: This definition is overly broad. At a minimum, this should be limited to first and last name and address in combination with one of (C) through (H). E.g. a zip code, by itself, should not be considered Personal Data.

Comment [pl4]: Should be limited to EDI vendors, or those that have access to Utility's systems. Cloud storage providers (e.g. Amazon Web Services) are not going to agree to these terms or sign any Representative Addendum.

Application of the terms in this Agreement should vary based on the specifics of the application by the Third Party Representative. For example, EDI providers have different access and risk than marketing contractors and/or brokers. One size does - and should not - fit all.

Date to all Confidential Utility Information disclosed to Third Party by Utility or to which Third Party is given access by Utility, including all archival or back-up copies of the Confidential Utility Information

held or maintained by Third Party (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, and all correspondence between or among the Parties or their respective Representatives pertaining to the same shall constitute Confidential Utility Information hereunder.~~ No customer financial account information will be provided pursuant to this Agreement. If any information is inadvertently sent to Third Party, Third Party will ~~immediately~~ promptly notify the Utility and Destroy any such information in the appropriate manner. Third Party, and its Third Party Representatives, shall have a grace period of twelve (12) months from the Effective Date of this Agreement in which to cure any deficiencies with respect to its obligations under this Agreement, provided that Third Party and its Third Party Representatives work diligently and in good faith to come into compliance during such grace period.

Comment [pl5]: This conflicts with the definition of Confidential Utility Information provided above and unnecessarily expands the scope to information that is beyond that sought to be protected and so is therefore unreasonable.

3. **Third Party Compliance with all Applicable Commission Uniform Business Practices.**

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

Third Party 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.

Third Party is a vendor, agent or other entity providing services to an ESCO or DER.

Comment [pl6]: Companies that fall under this category are presumably Third Party Representatives to ESCOs. As such why would such entities have to BOTH execute a DSA and a Third Party Representative Agreement? These provisions are circular.

4. **Customer Consent.** Third Party warrants that it has obtained informed consent from all customers about whom Third Party requests ~~data~~ Confidential Utility Information and that it will retain such consent for a period of at least six years. Third Party agrees to provide proof of customer consent at the request of Utility and Utility reserves its right to audit Third Party for compliance with consent requirements herein. Third Party agrees that upon a customer revocation of consent, Third Party warrants that it will no longer access said customer's Confidential Utility ~~i~~Information and that it will Destroy any of said customer's Confidential Utility ~~I~~information in its or its Representative's possession.

Comment [pl7]: This sentence suggests that ESCOs cannot hold CUI. Was this sentence meant to say something else? For example, what is the notice mechanism?

5. **Provision of Information.** Utility agrees to provide to Third Party or its Representatives, certain Confidential Utility Information, as requested, provided that (A) Third Party and its Representatives are in compliance with the terms of this Agreement; (B) if required by Utility, Third Party has provided and has caused its Representatives to provide, to the satisfaction of Utility ~~any~~ the Vendor Product/Service Security Assessment~~s,~~ attached hereto as Exhibit A or such other risk assessment forms as Utility may reasonably require from time to time, but not more than once per year ("Assessment") and Third Party will comply with the Utility Assessment requirements as negotiated by the Parties; (C) Third Party (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as detailed in the Assessment and reasonably acceptable to Utility to protect Confidential Utility Information; and (D) Third Party complies and shall cause its Third-Party Representatives to comply with ~~Utility's data~~

Comment [pl8]: It is not clear which specific provisions flow down to Third Party Representatives.

Comment [pl9]: There is no Exhibit A. Is this meant to refer to the "Self-Attestation of Information Security Controls"? If so, this paragraph should be updated to align with the Self-Attestation of Information Security Controls.

Comment [pl10]: Please define these or remove.

~~protection programs~~the agreed-upon Assessment requirements. Provided the foregoing prerequisites have been satisfied, Third Party shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to Third Party. Data and/or

~~C~~confidential ~~I~~information will at all times remain the sole property of the Party collecting the data and/or ~~C~~confidential ~~I~~information. Nothing in this ~~Rider~~ 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 ~~D~~data and/or ~~C~~confidential ~~I~~information of the other Party.

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

7. **Exceptions Allowing Third Party to Disclose Confidential Utility Information.**

a. **Disclosure to Representatives**. Notwithstanding the provisions of Section 6 herein, Third Party may disclose Confidential Utility Information to its ~~contractors or subcontractors~~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 Representative ~~first~~ (A) is advised by Third Party of the sensitive and confidential nature of such Confidential Utility Information; (B) agrees to comply with the provisions of this Agreement~~, provided that with respect to Representatives and this subsection (B), such Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Representatives were Third Party~~; and (C) signs the Representative Agreement. ~~All such written agreements with Representatives shall include direct liability for the Representatives towards Utility for breach thereof by the Representatives, and a copy of such agreement and each~~The Representative Agreement and ~~Third Party agreement~~ shall be made available to Utility upon request. ~~Notwithstanding the foregoing, Third Party shall be liable to Utility for any act or omission of a Representative, including without limitation,~~

Comment [pl11]: Should be mutual, covering ESCO information flowing back to Utility.

Comment [pl12]: Services are not defined in the Recitals.

Comment [pl13]: Is this being required?

Comment [pl14]: There is no Exhibit B. Please provide for comment.

Comment [pl15]: Individual employees should not be required to sign anything.

Comment [pl16]: There is no Representative Agreement attached.

~~Representatives that would constitute a breach of this Agreement if committed by Third Party.~~

b. **Disclosure if Legally Compelled**. Notwithstanding anything herein, in the event that Third Party or any of its 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), Third Party shall, except to the extent prohibited by law, ~~within 24 hours~~promptly notify Utility, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, Utility shall have the right to consult with Third Party 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, Third Party and its 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 Third Party and its 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**. Within ~~ten~~ thirty (~~10~~30) days after Utility's written demand based upon a good faith business reason, Third Party shall (and shall cause its Representatives to) take reasonable steps 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~~,~~ and format that the Confidential Utility Information was provided to Third Party, and in such 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 Third Party's or its Representatives' possession as a result of the Utility and as set forth herein, including destroying Confidential Utility Information from all systems, records, archives, and backups of Third Party and its Representatives, and all subsequent ~~access, use, and~~ Processing of the Confidential Utility Information by Third Party and its Representatives shall cease. Notwithstanding the foregoing, Third Party and its 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, or as required by law, provided that Third Party and its Representatives shall ~~(1) not have experienced a Data Security Incident, (~~2~~1~~) not permit access to or recovery of Confidential Utility Information from such computer backup system and (~~3~~2) keep all such Confidential Utility Information confidential in accordance with this Agreement. Third Party shall, upon request, certify to Utility that the destruction by Third Party and its Representatives required by this Section has occurred by (A) having a duly authorized officer of Third Party complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Representatives

Comment [pl17]: 10 days is unreasonable, especially when accounting for (potentially) multiple layers of Representatives.

Comment [pl18]: Utility can ask ESCO to delete data at any time without reason, effectively shutting the ESCO down? This is unreasonable. There needs to be a legitimate reason for Utility to request the return or destruction of information.

Comment [pl19]: A minor Data Security Incident (e.g. inadvertent corruption of data) would preclude the allowance of backups? This is unreasonable.

and maintaining them on file. Compliance with this Section 8 shall not relieve Third Party from compliance with the other provisions of this Agreement. The obligations under this Section shall survive any expiration of termination of this Agreement.

9. **Audit.** Upon reasonable notice to Third Party, Third Party shall, and shall require its Representatives to permit Utility~~, its~~ auditors~~,~~ or designated audit representatives~~, and regulators~~ to audit and inspect, at Utility's sole expense ~~(except as otherwise provided in this Agreement)~~, and no more often than once per year (unless otherwise required by Utility's regulators): (A) the facilities of Third Party and Third Party's Representatives where Confidential Utility Information is Processed by or on behalf of Third Party; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) Third Party'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~~, at a minimum,~~ solely for the purpose of verifying Third Party's compliance with this Agreement, including all applicable Data Protection Requirements. Notwithstanding the generality of the foregoing, the audited party shall not be required to provide access to records to the extent that such access is prohibited by applicable law or if such records are legally privileged or outside the scope of verifying compliance with this Agreement. In addition, and notwithstanding the foregoing or anything else in this Agreement, the audit must be conducted pursuant to the parameters of the audited party's own policies, standards, and procedures for information security risk assessments. Notwithstanding anything herein, in the event of a Data Security Incident, Third Party shall and shall cause its Representatives to permit an audit hereunder more frequently than once per year, as may be reasonably requested by Utility. Third Party shall ~~immediately~~ promptly correct any deficiencies reasonably identified by Utility.

10. **Investigation.** Upon reasonable notice to Third Party, Third Party shall assist and support Utility where reasonable in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to a Data Security Incident involving Confidential Utility Information Processed by Third Party on behalf of Utility, and without waiver by ESCO of any rights or privileges under applicable law. Such assistance shall be at Utility's sole expense, except where such investigation was required solely due to the proven acts or omissions of Third Party or its Representatives, in which case such assistance shall be at Third Party's sole expense.

11. **Data Security Incidents.** Third Party is responsible for any and all Data Security Incidents caused by Third Party or its Representatives involving Confidential Utility Information that is Processed by~~, or on behalf of,~~ Third Party or its Representatives. Third Party shall, except as otherwise required by law, promptly notify Utility in writing ~~immediately~~ (and in any event within ~~twenty-four (24) hours~~five (5) business days) whenever Third Party reasonably believes that there has been a Data Security Incident. The notification required by this Section 11 may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation, and such notification shall only be made after such law enforcement agency determines that such notification does not compromise such investigation. After providing such notice, Third Party will investigate the Data Security Incident, and ~~immediately~~ promptly take ~~all necessary~~reasonable 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~~. Third Party further agrees to provide, at Third Party's sole cost,

Comment [pl20]: This is unreasonable, especially considering how broadly Third Party Representatives is defined. Certain vendors may not be agreeable to this. Vendors may object to being subjected to an audit by parties that they are not in contract with.

Comment [pl21]: What data security provisions are in place for these auditors to protect and secure information obtained about ESCO data, systems, security, etc. What insurance is in place? Will ESCOs be additional insureds? Where will the information be stored? How secured?

Comment [pl22]: Needs to be defined further (see comment to definition).

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, Third Party shall not notify any individual ~~or any third party~~ other than law enforcement or third parties protected under attorney-client privilege of any ~~potential~~ Data Security Incident involving Confidential Utility Information without first ~~consulting with~~ disclosing to, and obtaining the permission of, Utility, such permission not to be unreasonably withheld, conditioned or delayed. In addition, within 30 days of ~~identifying or being informed~~notification to Utility of a Data Security Incident, Third Party shall

develop and execute a plan, those unprivileged or protected portions subject to Utility's reasonable approval, that reduces the likelihood of a recurrence of such Data Security Incident. Third Party agrees that Utility may at its reasonable discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a subsequent Data Security Incident occurs.

12. **Cybersecurity Insurance Required.** Third Party shall carry and maintain ~~C~~cybersecurity insurance in an amount of no less than $~~10~~2,~~05~~00,000 per incident and Utility shall be included by endorsement as an additional insured on Third Party's ~~C~~cybersecurity insurance. Third Party agrees to cause its ~~Contractors~~ Representatives to carry and maintain cybersecurity insurance in the amount shown above.

13. **No Intellectual Property Rights Granted.** Except as otherwise set forth herein or agreed to in writing by the Parties, ~~N~~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 Third Party shall acquire no ownership interest in the Confidential Utility Information (which, as between Third Party 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 Agreement.

14. **Additional Obligations.**

a. Third Party shall not create or maintain data which are derivative of Confidential Utility Information except for a legitimate business purpose, such as for the purpose of performing its obligations under this Agreement or as authorized by Utility. ~~Data collected by Third Party from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with Third Party or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Agreement.~~

b. Third Party 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 Third Party to be applicable to Utility~~.

c. Third Party 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 Third Party's internal use, Processing, or other transmission of Confidential Utility Information, whether between or among Third Party's Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of Third Party, including without limitation Representatives.

d. Third Party shall ~~safely~~ reasonably secure or encrypt all Confidential Utility Information during storage or transmission.

e. Third Party shall establish policies and procedures to provide reasonable and prompt

Comment [pl23]: Utility should make a tariff amendment before it can require insurance in an amount that will directly impact customer pricing. Such a requirement may result in "unreasonable or burdensome" costs. Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25; *See also* Case 96-E-0909, Matter of Central Hudson Gas & Electric Corporation's Plans for Electric Rate/Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 22.

Comment [pl24]: $10M is not industry standard for this type of data.

Comment [pl25]: It is unreasonable to flow this down to all Third Party Representatives, considering how broadly this is defined. This is also unnecessarily redundant. There will be different levels of Third Party Representatives with different levels of access. Terms flowed down should vary. An EDI vendor is different than a marketing vendor/broker with limited access to CUI.

Comment [pl26]: Moved to definition section.

Comment [pl27]: Needs to be defined further (see comment to definition).

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 Third Party to the extent such request, complaint or other communication relates to Third Party's Processing of such individual's Confidential Utility Information.

f. Third Party 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~~has an interest in the ~~Confidential Utility Information, data~~ theft~~,~~ or other unauthorized release, disclosure or misuse 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 Third Party's ~~accessing or~~ Processing of such Confidential Utility Information.

15. Payment. In consideration of Utility's agreement to provide Confidential Utility Information in accordance with Section 2, Third Party shall pay to Utility fees pursuant to its tariffs.

16. 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 the provision or Processing of Confidential Utility Information hereunder. Third Party 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 and Limitation of Liability. To the fullest extent permitted by law, ~~Third Party~~each Party shall indemnify and hold ~~Utility~~the other Party, 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 ~~Third Party or any of its Representatives~~such Party. Notwithstanding anything to the contrary, in no event shall any Party be liable for or entitled to indirect, special, punitive, (including but not limited to any loss for anticipated revenue, earnings or profits, lost opportunity or increased expense or operations) or consequential damages whether by statute, in contract, or tort pursuant to or in connection with this Addendum and all such damages are hereby expressly disclaimed and waived.

18. Notices. With the exception of notices or correspondence relating to potential or pending

Comment [pl28]: To the extent Utility shares any liability that may be gross negligence or willful misconduct, the limitation may be prohibited under 16 NYCRR 218.1. *See also* Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25.

Comment [pl29]: The miscellaneous provisions should correspond any existing agreement with Con Ed.

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 Third Party, to:

Third Party Name:
Name of Contact:
Address:
Phone:
Email:

If to Utility, to:

Utility Name: Consolidated Edison Company of New York, Inc.
Name of Contact: Jason Miller
Address: 4 Irving Place, 9th Fl, New York, NY 10003
Phone: 212-780-6702
Email: MILLERJAS@CONED.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 Agreement shall be effective as of the date first set forth above and shall remain in effect ~~until~~ unless terminated by Utility or Third Party ~~upon not less than 10 days' prior written notice specifying the effective date of termination,~~ for material breach by the other Party; 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~~; and provided, further, that Utility may terminate this Agreement immediately upon notice to Third Party in the event of a material breach hereof by Third Party or its Representatives~~. For the purpose of clarity, a breach of Sections 3-~~4, 6-~~11, 13-14, 17, and 25 shall be a material breach hereof. Upon the expiration or termination hereof, neither Third Party nor its Representatives shall have any further right to Process Confidential Utility Information and shall ~~immediately~~ promptly comply with its obligations under Section 8.

Comment [pl30]: The term should run concurrent with any existing Con Ed contract.

Comment [pl31]: Section references are not consistent across all DSAs.

20. **Consent to Jurisdiction; Selection of Forum**. ~~Third Party~~The Parties irrevocably submit~~s~~ 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 Agreement. ~~Third Party~~The Parties agree~~s~~ that service of process on a Party~~it~~ in relation to such jurisdiction may be made by certified or registered mail addressed to ~~Third Party~~the served Party at the address for ~~Third Party~~ such Party pursuant to Section ~~11~~ 18 hereof, which will be effective upon actual receipt by served Party ~~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~~. ~~Third Party~~Parties agree~~s~~ that service of process ~~on it~~ may also be made in any manner permitted by law. ~~Third Party~~Parties consent~~s~~ to the selection of the New York State and

United States courts within New York County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement, unless otherwise required by law. Nothing in this Section 20 shall diminish or circumvent the dispute resolution rights and obligations, or the procedure for dispute resolution pursuant to Section 33 of this Agreement.

21. **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.

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

23. **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.

24. **Amendments; Waivers.** 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.

25. **Assignment.** This Agreement ~~(and Aggregator's obligations hereunder)~~ may not be assigned by ~~Third Party or Representatives~~either Party without the prior written consent of ~~Utility~~the other Party, and any purported assignment without such consent shall be void. Such consent shall not be unreasonably withheld, conditioned or delayed.

26. **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.

27. **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.

28. **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.

29. **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 other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, ~~or~~ communications failure, or governmental action or order) 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.

30. **Relationship of the Parties.** Utility and Third Party 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.

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

32. **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.

~~32.~~33. **Dispute Resolution.** Each Party shall use its best efforts to resolve any dispute related to this Agreement between them promptly and amicably and without resort to any legal process if feasible within thirty (30) days of receipt of a written notice by one Party to the other Party of the existence of such dispute. The dispute resolution process in Section 8 of the Uniform Business Practices ("UBP") is incorporated as if set forth fully herein. In addition to UBP Section 8, Third Party may also seek relief from the Public Service Commission pursuant to its reserved authority over Utility-ESCO operating agreements for purposes of dispute resolution. 98-E-0952 - Matter of Competitive Opportunities Regarding Electric Service, Statement of Regulatory Policies Regarding Operating Agreements (issued Mar. 10, 1998).

[signature page follows]

Comment [pl32]: *See also* 96-E-0909 - Matter of Central Hudson Gas & Electric Corporation's Plans for Electric/Rate Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 21 & n.1 (citing to Statement of Regulatory Policy, and referencing previously reserved authority to resolve disputes for both operating agreements and handbooks).

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

By: _____	By: _____
Name: _____	Name:
Title:	Title: Matthew Sexton
	General Manager, Specialized Activities

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

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, unless otherwise required or prevented by law, 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~~in accordance with the terms of the Addendum.

_____ Role-based access controls are used to restrict system access to authorized users and limited ~~on a need to know basis~~based on job function or other legitimate business reason.

_____ 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, unless there is a reasonable basis not to do so. 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, unless

_____ impracticable.

_____ 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 if they contain Confidential Utility Information.

~~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,~~ solely 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

Comment [pl33]: Audit scope needs to be defined and coordinated between provisions of the Agreement. There should not be three audit provisions.

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: _____

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___ (the "Effective Date") by and between Rochester Gas & Electric 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

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, 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. Confidential Utility Information shall not include any information of ESCO/DC which: (A) was in the public domain at the time of disclosure by Utility to ESCO/DC; (B) became part of the public domain after disclosure by Utility to ESCO through no fault of ESCO/DC; (C) was acquired by ESCO/DC independently after disclosure by Utility to ESCO/DC, from a third party without breach of agreement or violation of law; or (D) was in ESCO's/DC's possession prior to the time of disclosure by Utility to ESCO/DC. For avoidance of doubt, 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. "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; (B) the Utility's internal requirements and procedures that are provided by Utility to ESCO/DC 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; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by ESCO/DC or any current or former Representatives. Good faith acquisition of Confidential Utility Information by an employee or agent of ESCO/DC for the purposes of the business is not a Data Security Incident, provided that the Confidential Utility Information is not misused or subject to unauthorized disclosure.

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, except as otherwise required by law, including but not limited to record retention requirements and litigation holds.

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; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial, or health information; or (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, including Social Security number, passport number, driver's license number, Utility customer account number, Municipal Identification (NYCID), or similar identifier.

j. "Third-Party Representatives" or "Representatives" means those agents of ESCO/DC that are Electronic Data Interchange vendors, contractors or subcontractors.

Comment [pl1]: An inadvertent corruption of data could be a normal business event fixed through routine backup procedures. This should not be deemed a Data Security Incident.

Comment [pl2]: Same comment as above

Comment [pl3]: This definition is overly broad. At a minimum, this should be limited to first and last name and address in combination with one of (C) through (H). E.g. a zip code, by itself, should not be considered Personal Data.

Comment [pl4]: Should be limited to EDI vendors, or those that have access to Utility's systems. Cloud storage providers (e.g. Amazon Web Services) are not going to agree to these terms or sign any Representative Addendum.

Application of the terms in this Agreement should vary based on the specifics of the application by the Third Party Representative. For example, EDI providers have different access and risk than marketing contractors and/or brokers. One size does - and should not - fit all.

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

2. **Scope of the Addendum.** This Addendum shall govern and apply as of the Effective Date to all Confidential Utility Information disclosed to ESCO/DC by Utility 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 customer financial account information will be provided pursuant to this Addendum. If any information is inadvertently sent to ESCO/DC, ESCO/DC will ~~immediately~~ promptly notify the Utility and Destroy any such information in the appropriate manner. ESCO/DC, and its Third Party Representatives, shall have a grace period of twelve (12) months from the Effective Date of this Addendum in which to cure any deficiencies with respect to its obligations under this Addendum, provided that ESCO/DC and its Third Party Representatives work diligently and in good faith to come into compliance during such grace period.

Comment [pl5]: This conflicts with the definition of Confidential Utility Information provided above and unnecessarily expands the scope to information that is beyond that sought to be protected and so is therefore unreasonable.

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.

Comment [pl6]: Companies that fall under this category are presumably Third Party Representatives to ESCOs. As such why would such entities have to BOTH execute a DSA and a Third Party Representative Agreement? These provisions are circular.

4. **Customer Consent.** ESCO/DC warrants that it has obtained informed consent from all customers about whom ESCO/DC requests ~~data~~ Confidential Utility Information 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 Confidential Utility ~~i~~Information and that it will Destroy any of said customer's Confidential Utility ~~i~~Information in its or its Representative's possession.

Comment [pl7]: This sentence suggests that ESCOs cannot hold CUI. Was this sentence meant to say something else? For example, what is the notice mechanism?

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

Comment [pl8]: It is not clear which specific provisions flow down to Third Party Representatives.

its Representatives to provide, to the satisfaction of Utility ~~any~~ the Vendor Product/Service Security Assessment~~s,~~ attached hereto as Exhibit A or such other risk assessment forms as Utility may reasonably require from time to time, but not more than once per year ("Assessment") and ESCO/DC will comply with the Utility Assessment

Comment [pl9]: Is this meant to refer to the "Self-Attestation of Information Security Controls"? If so, this paragraph should be updated to align with the Self-Attestation of Information Security Controls.

Comment [pl10]: Please define these or remove.

requirements as negotiated by the Parties; (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 and 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~~ the agreed-upon Assessment requirements. 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. Data and/or ~~C~~confidential ~~I~~information will at all times remain the sole property of the Party collecting the data and/or ~~C~~confidential ~~I~~information. Nothing in this ~~Rider~~ Addendum 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 ~~D~~data and/or ~~C~~confidential ~~I~~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) 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~~C) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Addendum; (~~E~~D) limit reproduction of Confidential Utility Information; (~~F~~E) 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~~F) 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~~G) to the extent required by the Utility, each ~~person with a need to know the Confidential Information~~Representative 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~~ reasonable 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.

Comment [pl11]: Should be mutual, covering ESCO information flowing back to Utility.

Comment [pl12]: Services are not defined in the Recitals.

Comment [pl13]: Is this being required?

Comment [pl14]: Individual employees should not be required to sign anything.

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 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~~The 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.~~

Comment [pl15]: Individual employees should not be required to sign anything.

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 24 hours~~promptly notify Utility, 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. Within ~~ten~~ thirty (~~10~~30) days after Utility's written demand based upon a good faith business reason, ESCO/DC shall (and shall cause its Third Party Representatives to) take reasonable steps 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~~,~~ and format that the Confidential Utility Information was provided to ESCO/DC, and in such 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 as a result of the Utility and as set forth herein, including destroying Confidential Utility Information from all systems, records, archives, and backups of ESCO/DC and its Third Party Representatives, and all

Comment [pl16]: 10 days is unreasonable, especially when accounting for (potentially) multiple layers of Representatives.

Comment [pl17]: Utility can ask ESCO to delete data at any time without reason, effectively shutting the ESCO down? This is unreasonable. There needs to be a legitimate reason for Utility to request the return or destruction of information.

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, or as required by law, provided that ESCO/DC and its Third Party Representatives shall ~~(1) not have experienced a Data Security Incident,~~ (~~2~~1) not permit access to or recovery of Confidential Utility Information from such computer backup system and (~~3~~2) 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, or 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~~, at a minimum,~~ solely for the purpose of verifying ESCO/DC's compliance with this Addendum, including all applicable Data Protection Requirements. Notwithstanding the generality of the foregoing, the audited party shall not be required to provide access to records to the extent that such access is prohibited by applicable law or if such records are legally privileged or outside the scope of verifying compliance with this Addendum. In addition, and notwithstanding the foregoing or anything else in this Addendum, the audit must be conducted pursuant to the parameters of the audited party's own policies, standards, and procedures for information security risk assessments. 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 reasonably requested by Utility. ESCO/DC shall ~~immediately~~ promptly correct any deficiencies reasonably identified by Utility.

10. **Investigation.** Upon reasonable notice to ESCO/DC, ESCO/DC shall assist and support Utility where reasonable in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to a Data Security Incident involving Confidential Utility Information Processed by ESCO/DC on behalf of Utility, and without waiver by ESCO of any rights or privileges under applicable law. Such assistance shall be at Utility's sole

Comment [pl18]: A minor Data Security Incident (e.g. inadvertent corruption of data) would preclude the allowance of backups? This is unreasonable.

Comment [pl19]: This is unreasonable, especially considering how broadly Third Party Representatives is defined. Certain vendors may not be agreeable to this. Vendors may object to being subjected to an audit by parties that they are not in contract with.

Comment [pl20]: What data security provisions are in place for these auditors to protect and secure information obtained about ESCO data, systems, security, etc. What insurance is in place? Will ESCOs be additional insureds? Where will the information be stored? How secured?

Comment [pl21]: Needs to be defined further (see comment to definition).

expense, except where such investigation was required solely due to the proven 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 caused by ESCO/DC or its Third Party Representatives involving Confidential Utility Information that is Processed by

~~, or on~~

~~behalf of,~~ESCO/DC or its Third Party Representatives. ESCO/DC shall, except as otherwise required by law, promptly notify Utility in writing ~~immediately~~ (and in any event within ~~twenty-four (24) hours~~five (5) business days) whenever ESCO/DC reasonably believes that there has been a Data Security Incident. The notification required by this Section 11 may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation, and such notification shall only be made after such law enforcement agency determines that such notification does not compromise such investigation. After providing such notice, ESCO/DC will investigate the Data Security Incident, and ~~immediately~~ promptly take ~~all necessary~~ reasonable 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 or third parties protected under attorney-client privilege, of any ~~potential~~ Data Security Incident involving Confidential Utility Information without first ~~consulting with~~ disclosing to, and obtaining the permission of, Utility, such permission not to be unreasonably withheld, conditioned or delayed. In addition, within 30 days of ~~identifying or being informed~~ notification to Utility of a Data Security Incident, ESCO/DC shall develop and execute a plan, those unprivileged or protected portions subject to Utility's reasonable approval, that reduces the likelihood of a recurrence of such Data Security Incident. ESCO/DC agrees that Utility may at its reasonable discretion and without penalty immediately suspend performance hereunder and/or terminate the Addendum if a subsequent Data Security Incident occurs.

12. Cybersecurity Insurance Required. ESCO/DC shall carry and maintain ~~C~~cybersecurity insurance in an amount of no less than $~~10~~2,~~05~~00,000 per incident and Utility shall be included by endorsement as an additional insured on ESCO/DC's ~~C~~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. Except as otherwise set forth herein or agreed to in writing by the Parties, ~~N~~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.

Comment [pl22]: Utility should make a tariff amendment before it can require insurance in an amount that will directly impact customer pricing. Such a requirement may result in "unreasonable or burdensome" costs. Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25; *See also* Case 96-E-0909, Matter of Central Hudson Gas & Electric Corporation's Plans for Electric Rate/Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 22.

Comment [pl23]: $10M is not industry standard for this type of data.

Comment [pl24]: It is unreasonable to flow this down to all Third Party Representatives, considering how broadly this is defined. This is also unnecessarily redundant. There will be different levels of Third Party Representatives with different levels of access. Terms flowed down should vary. An EDI vendor is different than a marketing vendor/broker with limited access to CUI.

14. Additional Obligations.

a. ESCO/DC shall not create or maintain data which are derivative of Confidential Utility Information except for a legitimate business purpose, such as 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.~~

Comment [pl25]: Moved to definition section.

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~~.

Comment [pl26]: Needs to be defined further (see comment to definition).

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~~ reasonably 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~~has an interest in the ~~Confidential Utility Information, data~~ theft~~,~~ or other unauthorized release, disclosure or misuse 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 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 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 and Limitation of Liability.** To the fullest extent permitted by law, ~~ESCO/DC~~each Party shall indemnify and hold ~~Utility~~the other Party, 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 Addendum by ~~ESCO/DC or any of its Third Party Representatives~~such Party. Notwithstanding anything to the contrary, in no event shall any Party be liable for or entitled to indirect, special, punitive, (including but not limited to any loss for anticipated revenue, earnings or profits, lost opportunity or increased expense or operations) or consequential damages whether by statute, in contract, or tort pursuant to or in connection with this Addendum and all such damages are hereby expressly disclaimed and waived.

Comment [pl27]: To the extent Utility shares any liability that may be gross negligence or willful misconduct, the limitation may be prohibited under 16 NYCRR 218.1. *See also* Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25.

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:

Comment [pl28]: The miscellaneous provisions should correspond any existing agreement with RG&E.

If to ESCO/DC, to:

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

If to Utility, to:

Rochester Gas & Electric 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~~ unless terminated by Utility or ESCO/DC ~~upon not less than 10 days' prior written notice specifying the effective date of termination~~for material breach by the other Party, 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~~ promptly comply with its obligations under Section 8.

Comment [pl29]: The term should run concurrent with any existing RG&E contract.

Comment [pl30]: Section references are not consistent across all DSAs.

20. **Consent to Jurisdiction; Selection of Forum**. ~~ESCO/DC~~The Parties irrevocably submit~~s~~ 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~~The Parties agree~~s~~ that service of process on ~~it in~~a Party in relation to such jurisdiction may be made by certified or registered mail addressed to ~~ESCO/DC~~the served Party at the address for ~~ESCO/DC~~such Party pursuant to Section ~~11~~ 18 hereof, which will be effective upon actual receipt by served Party ~~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~~Parties agree~~s~~ that service of process ~~on it~~ may also be made in any manner permitted by law. ~~ESCO/DC~~Parties consent~~s~~ 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, unless otherwise required by law. Nothing in this Section 20 shall diminish or circumvent the dispute resolution rights and obligations, or the procedure for dispute resolution pursuant to Section 33 of 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 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~~either Party without the prior written consent of ~~Utility~~the other Party, and any purported assignment without such consent shall be void. Such consent shall not be unreasonably withheld, conditioned or delayed.

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~~ agreement 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, or governmental action or order) 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. Dispute Resolution. Each Party shall use its best efforts to resolve any dispute related to this Addendum between them promptly and amicably and without resort to any legal process if feasible within thirty (30) days of receipt of a written notice by one Party to the other Party of the existence of such dispute. The dispute resolution process in Section 8 of the Uniform Business Practices ("UBP") is incorporated as if set forth fully herein. In addition to UBP Section 8, Third Party may also seek relief from the Public Service Commission pursuant to its reserved authority over Utility-ESCO operating agreements for purposes of dispute resolution. 98-E-0952 - Matter of Competitive Opportunities Regarding Electric Service, Statement of Regulatory Policies Regarding Operating Agreements (issued Mar. 10, 1998).

[Signature page follows]

Comment [pl31]: *See also* 96-E-0909 - Matter of Central Hudson Gas & Electric Corporation's Plans for Electric/Rate Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 21 & n.1 (citing to Statement of Regulatory Policy, and referencing previously reserved authority to resolve disputes for both operating agreements and handbooks).

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

Rochester Gas and Electric Corporation	ESCO/DC
By: _____	By: _____
Name:_____	Name: _____
Title:	Title:

EXHIBIT A

Comment [pl32]: To be replaced by document entitled, "Self-Attestation of Information Security Controls".

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 Utility 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 Utility 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 Utility Information or (b) a violation of an explicit or implemented ~~C~~company security policy.

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

Comment [pl33]: Why not use the definition of Data Security Incident in the Addendum?

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 Utility Information will at all times remain the sole property of the Party collecting the ~~d~~Data and/or Confidential Utility 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 ~~C~~confidential ~~i~~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~~ Confidential Utility Information ("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 reasonably sufficient to Utility, regarding the state of the internal control environment of the Third Party Representative to enable Utility to perform ~~any~~ a reasonable 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 reasonable requirements, provided that such requirements shall not be any more restrictive than those set forth in the Addendum.

Comment [pl34]: 20 days may be overly burdensome in certain instances.

(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~~ reasonable 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~~ the exchange of Confidential Utility Information 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~~ Confidential Utility Information 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~~standards 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~~ Confidential Utility Information according to industry recognized ~~best practices~~standards 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~~ Confidential Utility Information during storage or transmission.

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

~~vii.~~vi. Except as may be necessary in connection with the ~~data~~ exchange of Confidential Utility Information, 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~~ Confidential Utility Information, 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~~ reasonable 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 ~~d~~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.~~i. 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.~~ii. Upon Utility's request, ESCO/DC and each Third Party Representative shall promptly provide the results of any vulnerability assessment and penetration test.

~~vi.~~iii. 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.

Comment [pl35]: Obligations under II(5) should be sufficient.

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 required security activities have been performed, and all identified security issues have been documented and resolved.

(2) ESCO/DC warrants, to its knowledge, 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 Utility Information, Data or other information technology resource. ESCO/DC warrants that, to its knowledge, 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.

Comment [pl36]: To be discussed regarding technical capabilities of application interface.

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)~~(1) 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)~~(2) ESCO/DC and their Third Party Representative(s) shall notify Utility of a ~~c~~Cyber ~~-i~~Incident based on the ~~Notification Table~~ notification obligations set forth in the Addendum. ~~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~~

Comment [pl37]: ESCO is not a software as a service provider. There are no uptime guarantees. These reporting obligations conflict with the reporting obligations in the Addendum. The inclusion of this chart is unreasonable.

(4) ESCO/DC and its Third Party Representative(s) shall establish policies and procedures to properly investigate a Cyber Event or Cyber Incident caused by ESCO/DC or its Third Party Representative 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~~ Confidential Utility Information and to ensure that ESCO/DC's Third ~~p~~Party Representatives' information systems related to the data exchange are operating effectively to ensure availability. The evidence may include, as reasonably 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 ~~p~~Party Representative(s) are in compliance~~, such as an ISO 27001 or PCI DSS certification letter~~.

Utility may also, at its cost and subject to reasonable 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 ~~C~~contracts with each of its Third Party Representative(s) a corresponding right for Utility to audit their services. ESCO/DC is responsible for addressing ~~any~~ reasonable user entity control requirements and ~~any~~ control deficiencies or findings that are noted in these audit reports.

Comment [pl38]: This provision conflicts with the Audit provisions in the Addendum and in the Attestation. There should not be three separate audit provisions.

Comment [pl39]: This is unreasonable.

EXHIBIT B

THIRD-PARTY REPRESENTATIVE ADDENDUM

I, _____ , have read the Addendum between _____, ("Company") and Rochester Gas & Electric 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 Utility Information disclosed by Utility to the ESCO/DC pursuant to the Addendum.

Comment [pl40]: This should be ESCO/DC to match Addendum definition.

_____ _____

Signature Date

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

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").

Comment [pl41]: This should be ESCO/DC to match Addendum definition.

WHEREAS, Third Party desires to retain access to certain Confidential Utility Information (as defined previously in this ~~Data Security Agreement~~Addendum), 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, unless otherwise required or prevented by law, 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~~in accordance with the terms of the Addendum.

_____ Role-based access controls are used to restrict system access to authorized users and limited ~~on a need-to-know basis~~based on job function or other legitimate business reason.

_____ 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, unless there is a reasonable basis not to do so. 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, unless

_____ impracticable.

_____ 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 if they contain Confidential Utility Information.

~~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,~~ solely 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

Comment [pl42]: Audit scope needs to be defined and coordinated between provisions of the Addendum. There should not be three audit provisions.

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: _____

DATA SECURITY ADDENDUM

This Data Security Addendum ("Addendum") to the Retail Supplier Operating Agreement (Electric or Gas) effective January 11, 2012, is made and entered into this _____ day of ___ , 20___ (the "Effective Date") by and between Central Hudson Gas & Electric Corporation, a New York corporation with offices at 284 South Avenue, Poughkeepsie, New York 12601 ("Utility") and _____., an Energy Services Company ("ESCO") 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 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 aggregated customer information; and

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

WHEREAS, Utility and ESCO also desire to enter into this Addendum to establish, among other things, the full scope of ESCO'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, collectively, aggregated and customer-specific information that Utility is: (A) required by the Commission to provide to ESCO and (B) any other Utility-specific, aggregated, Personal Data, Sensitive Data, or Utility Data, or customer-specific data provided to ESCO by Utility. Confidential Utility Information shall not include any information of ESCO which: (A) was in the public domain at the time of disclosure by Utility to ESCO; (B) became part of the public domain after disclosure by Utility to ESCO through no fault of ESCO; (C) was acquired by ESCO independently after disclosure by Utility to ESCO, from a third party without breach of agreement or violation of law; or (D) was in ESCO's possession prior to the time of disclosure by Utility to ESCO. For avoidance of doubt, data collected by ESCO from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESCO or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Addendum.

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 or its Representative’s Processing of Confidential Utility Information; (B) the Utility’s internal requirements and procedures that are provided by Utility to ESCO relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESCO 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 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; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by ESCO or any current or former Representatives. Good faith acquisition of Confidential Utility Information by an employee or agent of ESCO for the purposes of the business is not a Data Security Incident, provided that the Confidential Utility Information is not misused or subject to unauthorized disclosure.

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, except as otherwise required by law, including but not limited to record retention requirements and litigation holds.

e. "ESCO" 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; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial, or health information; or (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, including Social Security number, passport number, driver's license number, Utility customer account number, Municipal Identification (NYCID), or similar identifier.

Comment [pl1]: An inadvertent corruption of data could be a normal business event fixed through routine backup procedures. This should not be deemed a Data Security Incident.

Comment [pl2]: Same comment as above

Comment [pl3]: This definition is overly broad. At a minimum, this should be limited to first and last name and address in combination with one of (C) through (H). E.g. a zip code, by itself, should not be considered Personal Data.

j. “Third-Party Representatives” or “Representatives” means those agents of ESCO that are Electronic Data Interchange vendors, contractors or subcontractors.

Comment [pl4]: Should be limited to EDI vendors, or those that have access to Utility’s systems. Cloud storage providers (e.g. Amazon Web Services) are not going to agree to these terms or sign any Representative Addendum.

Application of the terms in this Agreement should vary based on the specifics of the application by the Third Party Representative. For example, EDI providers have different access and risk than marketing contractors and/or brokers. One size does - and should not - fit all.

k. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of ESCO or a ~~ESCO~~ third party and whether or not it is provided to ESCO.

2. Scope of the Addendum. This Addendum shall govern and apply as of the Effective Date to all Confidential Utility Information disclosed to ESCO by Utility or to which ESCO is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by ESCO (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 customer financial account information will be provided pursuant to this Addendum. If any information is inadvertently sent to ESCO, ESCO will ~~immediately~~ promptly notify the Utility and Destroy any such information in the appropriate manner. ESCO, and its Third Party Representatives, shall have a grace period of twelve (12) months from the Effective Date of this Addendum in which to cure any deficiencies with respect to its obligations under this Addendum, provided that ESCO and its Third Party Representatives work diligently and in good faith to come into compliance during such grace period.

Comment [pl5]: This conflicts with the definition of Confidential Utility Information provided above and unnecessarily expands the scope to information that is beyond that sought to be protected and so is therefore unreasonable.

3. ESCO Compliance with all Applicable Commission Uniform Business Practices.

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

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

Comment [pl6]: Companies that fall under this category are presumably Third Party Representatives to ESCOs. As such why would such entities have to BOTH execute a DSA and a Third Party Representative Agreement? These provisions are circular.

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

Comment [pl7]: This sentence suggests that ESCOs cannot hold CUI. Was this sentence meant to say something else? For example, what is the notice mechanism?

5. **Provision of Information.** Utility agrees to provide to ESCO or its Representatives, certain Confidential Utility Information, as requested, provided that (A) ESCO and its Representatives are in compliance with the terms of this Addendum; (B) if required by Utility, ESCO has provided and has caused its Representatives to provide, to the satisfaction of Utility ~~any~~ the Vendor Product/Service Security Assessment~~s,~~ attached hereto as Exhibit A, or such other risk assessment forms as Utility may reasonably require from time to time, but not more than once per year ("Assessment") and ESCO will comply with the Utility Assessment requirements as negotiated by the Parties; (C) ESCO (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as detailed in the Assessment and reasonably acceptable to Utility to protect Confidential Utility Information; and (D) ESCO complies and shall cause its Third-Party Representatives to comply with ~~Utility's data protection programs~~the agreed-upon Assessment requirements. Provided the foregoing prerequisites have been satisfied, ESCO shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to ESCO. Data and/or ~~C~~confidential ~~I~~information will at all times remain the sole property of the Party collecting the data and/or ~~C~~confidential ~~I~~information. Nothing in this ~~Rider~~ Addendum 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 ~~D~~data and/or ~~C~~confidential ~~I~~information of the other Party.

6. **Confidentiality.** ESCO shall: (A) hold all Confidential Utility Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Utility Information to any other person or entity (including but not limited to Third Party Representatives, affiliates, or members of ESCO); ~~(C) not Process Confidential Utility Information outside of the United States;~~ (~~D~~C) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Addendum; (~~E~~D) limit reproduction of Confidential Utility Information; (~~F~~E) 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~~F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as ESCO 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~~G) to the extent required by the Utility, ~~each person with a need to know the Confidential Information~~each Representative 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~~ reasonable assurances that the foregoing restrictions and protections concerning Confidential Utility Information are being observed and ESCO shall be obligated to promptly provide Utility with the requested assurances.

7. **Exceptions Allowing ESCO to Disclose Confidential Utility Information.**

Comment [pl8]: It is not clear which specific provisions flow down to Third Party Representatives.

Comment [pl9]: Is this meant to refer to the "Self-Attestation of Information Security Controls"? If so, this paragraph should be updated to align with the Self-Attestation of Information Security Controls.

Comment [pl10]: Please define these or remove.

Comment [pl11]: Should be mutual, covering ESCO information flowing back to Utility.

Comment [pl12]: Services are not defined in the Recitals.

Comment [pl13]: Is this being required?

Comment [pl14]: Individual employees should not be required to sign anything.

a. **Disclosure to Representatives**. Notwithstanding the provisions of Section 6 herein, ESCO 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 of the sensitive and confidential nature of such Confidential Utility Information; (B) agrees to comply with the 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~~; 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~~The Third Party Representative Addendum ~~and ESCO Addendum~~ shall be made available to Utility upon request. ~~Notwithstanding the foregoing, ESCO 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.~~

b. **Disclosure if Legally Compelled.** Notwithstanding anything herein, in the event that ESCO 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 shall, except to the extent prohibited by law, ~~within 24 hours~~promptly notify Utility, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, Utility shall have the right to consult with ESCO 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 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 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. Within ~~ten~~ thirty (~~10~~30) days after Utility's written demand based upon a good faith business reason, ESCO shall (and shall cause its Third Party Representatives to) take reasonable steps to cease to ~~access and~~ Process Confidential Utility Information and shall at the Utility's

Comment [pl15]: Individual employees should not be required to sign anything.

Comment [pl16]: 10 days is unreasonable, especially when accounting for (potentially) multiple layers of Representatives.

Comment [pl17]: Utility can ask ESCO to delete data at any time without reason, effectively shutting the ESCO down? This is unreasonable. There needs to be a legitimate reason for Utility to request the return or destruction of information.

option: (A) return such Confidential Utility Information to Utility in such manner, and format that the Confidential Utility Information was provided to ESCO, and in such 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's or its Third Party Representatives' possession as a result of the Utility and as set forth herein, including destroying Confidential Utility Information from all systems, records, archives, and backups of ESCO and its Third Party Representatives, and all subsequent access, use, and Processing of the Confidential Utility Information by ESCO and its Third Party Representatives shall cease. Notwithstanding the foregoing, ESCO 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, or as required by law, provided that ESCO and its Third Party Representatives shall (1) not have experienced a Data Security Incident, (21) not permit access to or recovery of Confidential Utility Information from such computer backup system and (32) keep all such Confidential Utility Information confidential in accordance with this Addendum. ESCO shall, upon request, certify to Utility that the destruction by ESCO and its Third Party Representatives required by this Section has occurred by (A) having a duly authorized officer of ESCO 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 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, ESCO shall, and shall require its Third Party Representatives to permit Utility, its auditors, or 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 and ESCO's Third Party Representatives where Confidential Utility Information is Processed by or on behalf of ESCO; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESCO'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, at a minimum, solely for the purpose of verifying ESCO's compliance with this Addendum, including all applicable Data Protection Requirements. Notwithstanding the generality of the foregoing, the audited party shall not be required to provide access to records to the extent that such access is prohibited by applicable law or if such records are legally privileged or outside the scope of verifying compliance with this Addendum. In addition, and notwithstanding the foregoing or anything else in this Addendum, the audit must be conducted pursuant to the parameters of the audited party's own policies, standards, and procedures for information security

Comment [pl18]: A minor Data Security Incident (e.g. inadvertent corruption of data) would preclude the allowance of backups? This is unreasonable.

Comment [pl19]: This is unreasonable, especially considering how broadly Third Party Representatives is defined. Certain vendors may not be agreeable to this. Vendors may object to being subjected to an audit by parties that they are not in contract with.

Comment [pl20]: What data security provisions are in place for these auditors to protect and secure information obtained about ESCO data, systems, security, etc. What insurance is in place? Will ESCOs be additional insureds? Where will the information be stored? How secured?

Comment [pl21]: Needs to be defined further (see comment to definition).

risk assessments. Notwithstanding anything herein, in the event of a Data Security Incident, ESCO shall and shall cause its Third Party Representatives to permit an audit hereunder more frequently than once per year, as may be reasonably requested by Utility. ESCO shall ~~immediately~~ promptly correct any deficiencies reasonably identified by Utility.

10. **Investigation.** Upon reasonable notice to ESCO, ESCO shall assist and support Utility where reasonable in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to a Data Security Incident involving Confidential Utility Information Processed by ESCO on behalf of Utility, and without waiver by ESCO of any rights or privileges under applicable law. Such assistance shall be at Utility's sole expense, except where such investigation was required solely due to the proven acts or omissions of ESCO or its Representatives, in which case such assistance shall be at ESCO's sole expense.

11. **Data Security Incidents.** ESCO is responsible for any and all Data Security Incidents caused by ESCO or its Third Party Representatives involving Confidential Utility Information that is Processed by~~, or on behalf of,~~ ESCO or its Third Party Representatives. ESCO shall, except as otherwise required by law, promptly notify Utility in writing ~~immediately~~ (and in any event within ~~twenty-four (24) hours~~five (5) business days) whenever ESCO reasonably believes that there has been a Data Security Incident. The notification required by this Section 11 may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation, and such notification shall only be made after such law enforcement agency determines that such notification does not compromise such investigation. After providing such notice, ESCO will investigate the Data Security Incident, and ~~immediately~~ promptly take ~~all necessary~~reasonable 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 further agrees to provide, at ESCO'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 shall not notify any individual, ~~or any ESCO~~ other than law enforcement or third parties protected under attorney-client privilege, of any ~~potential~~ Data Security Incident involving Confidential Utility Information without first ~~consulting~~ disclosing to~~with~~, and obtaining the permission of, Utility, such permission not to be unreasonably withheld, conditioned or delayed. In addition, within 30 days of ~~identifying or being informed~~notification to Utility of a Data Security Incident, ESCO shall develop and execute a plan, those unprivileged or protected portions subject to Utility's reasonable approval, that reduces the likelihood of a recurrence of such Data

Security Incident. ESCO agrees that Utility may at its reasonable discretion and without penalty immediately suspend performance hereunder and/or terminate the Addendum if a subsequent Data Security Incident occurs.

12. Cybersecurity Insurance Required. ESCO shall carry and maintain ~~C~~cybersecurity insurance in an amount of no less than ~~$10,000,000~~$2,500,000 per incident and Utility shall be included by endorsement as an additional insured on ESCO's ~~C~~cybersecurity insurance. ESCO agrees to cause its Third Party Representatives to carry and maintain cybersecurity insurance in the amount shown above.

13. No Intellectual Property Rights Granted. Except as otherwise set forth herein or agreed to in writing by the Parties, ~~N~~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 shall acquire no ownership interest in the Confidential Utility Information (which, as between ESCO 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 shall not create or maintain data which are derivative of Confidential Utility Information except for a legitimate business purpose, such as for the purpose of performing its obligations under this Addendum or as authorized by Utility. ~~Data collected by ESCO from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESCO or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Addendum.~~

Comment [pl22]: Utility should make a tariff amendment before it can require insurance in an amount that will directly impact customer pricing. Such a requirement may result in "unreasonable or burdensome" costs. Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25; *See also* Case 96-E-0909, Matter of Central Hudson Gas & Electric Corporation's Plans for Electric Rate/Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 22.

Comment [pl23]: $10M is not industry standard for this type of data.

Comment [pl24]: It is unreasonable to flow this down to all Third Party Representatives, considering how broadly this is defined. This is also unnecessarily redundant. There will be different levels of Third Party Representatives with different levels of access. Terms flowed down should vary. An EDI vendor is different than a marketing vendor/broker with limited access to CUI.

Comment [pl25]: Moved to definition section.

b. ESCO 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 to be applicable to Utility~~.

c. ESCO 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's internal use, Processing, or other transmission of Confidential Utility Information, whether between or among ESCO's Third Party Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of ESCO, including without limitation Third Party Representatives.

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

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

f. ESCO 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~~has an interest in the ~~Confidential Utility Information, data~~ theft~~,~~ or other unauthorized release, disclosure or misuse 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'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 shall pay to Utility 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 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

Comment [pl26]: Needs to be defined further (see comment to definition).

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 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 and Limitation of Liability.** To the fullest extent permitted by law, ~~ESCO~~ each Party shall indemnify and hold ~~Utility~~the other Party, 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 Addendum by ~~ESCO or any of its Third Party Representatives~~such Party. Notwithstanding anything to the contrary, in no event shall any Party be liable for or entitled to indirect, special, punitive, (including but not limited to any loss for anticipated revenue, earnings or profits, lost opportunity or increased expense or operations) or consequential damages whether by statute, in contract, or tort pursuant to or in connection with this Addendum and all such damages are hereby expressly disclaimed and waived.

Comment [pl27]: To the extent Utility shares any liability that may be gross negligence or willful misconduct, this limitation may be prohibited under 16 NYCRR 218.1. *See also* Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25.

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:

Comment [pl28]: The miscellaneous provisions should correspond any existing agreement with Central Hudson.

If to ESCO, to:

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

If to Utility, to:

Central Hudson Gas & Electric Corporation
Name of Contact: Katherine McIntosh
Address: 284 South Avenue
Poughkeepsie, New York 12601
Phone: (845) 486-5496
Email: kmcintosh@cenhud.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~~ unless terminated by Utility or ESCO ~~upon not less than 10 days' prior written notice specifying the effective date of termination~~for material breach by the other Party, 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 in the event of a material breach hereof by ESCO or its Third Party Representatives~~. For the purpose of clarity, a breach of Sections ~~3-4, 6~~3-11, 13, 16, and 24 shall be a material breach hereof. Upon the expiration or termination hereof, neither ESCO nor its Third Party Representatives shall have any further right to Process Confidential Utility Information and shall ~~immediately~~ promptly comply with its obligations under Section 8.

Comment [pl29]: The term should run concurrent with any existing Central Hudson contract.

Comment [pl30]: Section references are not consistent across all DSAs.

20. **Consent to Jurisdiction; Selection of Forum**. ~~ESCO~~ The Parties irrevocably submit~~s~~ 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~~ The Parties agree~~s~~ that service of process on ~~it~~ a Party in relation to such jurisdiction may be made by certified or registered mail addressed to ~~ESCO~~ the served Party at the address for ~~ESCO~~ such Party pursuant to Section ~~11~~18 hereof, which will be effective upon actual receipt by served Party ~~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~~ Parties agree~~s~~ that service of process ~~on it~~ may also be made in any manner permitted by law. ~~ESCO~~ Parties consent~~s~~ 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, unless otherwise required by law. Nothing in this Section 20 shall diminish or circumvent the dispute resolution rights and obligations, or the procedure for dispute resolution pursuant to Section 33 of 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 under this Addendum shall continue for so long as ESCO and/or ESCO's Third Party Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all Addendums between ESCO 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 or Third Party Representatives~~either Party without the prior written consent of ~~Utility~~the other Party, and any purported assignment without such consent shall be void. Such consent shall not be unreasonably withheld, conditioned or delayed.

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~~ agreement 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, or governmental action or order) 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 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. **Dispute Resolution**. Each Party shall use its best efforts to resolve any dispute related to this Addendum between them promptly and amicably and without resort to any legal process if feasible within thirty (30) days of receipt of a written notice by one Party to the other Party of the existence of such dispute. The dispute resolution process in Section 8 of the Uniform Business Practices ("UBP") is incorporated as if set forth fully herein. In addition to UBP Section 8, Third Party may also seek relief from the Public Service Commission pursuant to its reserved authority over Utility-ESCO operating agreements for purposes of dispute resolution. 98-E-0952 - Matter of Competitive Opportunities Regarding Electric Service, Statement of Regulatory Policies Regarding Operating Agreements (issued Mar. 10, 1998).

Comment [pl31]: *See also* 96-E-0909 - Matter of Central Hudson Gas & Electric Corporation's Plans for Electric/Rate Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 21 & n.1 (citing to Statement of Regulatory Policy, and referencing previously reserved authority to resolve disputes for both operating agreements and handbooks).

[signature page follows]

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

CENTRAL HUDSON GAS & ELECTRIC CORPORATION _____

By: _____ By: _____

Name: _____ Name: _____

Title: _____ Title: _____

EXHIBIT A

Comment [pl32]: To be replaced by document entitled, "Self-Attestation of Information Security Controls".

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?

EXHIBIT A

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 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 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 in the event that ESCO is granted or has access, in any way, to ~~Utility's data and/or~~ Confidential Utility 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 Utility Information" has the meaning set forth in this Addendum.

iii. "Customer Information" means a Utility electric or gas delivery Utility or ESCO 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 Utility Information or (b) a violation of an explicit or implemented ~~C~~company security policy.

v. "Cyber Incident" means (a) the loss or misuse (by any means) of data and/or Confidential Utility Information; (b) the inadvertent, unauthorized and/or unlawful access, processing, corruption, modification, transfer, disclosure, sale or rental of Confidential Utility Information; or (c) any other act or omission that compromises the security, confidentiality, integrity, availability, or privacy of ~~data and or~~ Confidential Utility 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 Utility Information, (iii) computer programs, software and source codes, (iv) operating and maintenance manuals with respect to the exchange of information, and (v)

Comment [pl33]: Why not use the definition of Data Security Incident in the Addendum?

any other written or otherwise recorded information relating to Addendum Exhibit A; which are either annexed to or referred to in the Addendum or this Data Security Rider ("Rider") or required to be supplied by ESCO pursuant to the terms of the Addendum Exhibit A 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 in performance of any obligation pursuant to this Addendum, including any individual, firm or corporation that is an affiliate, agent, or assigned of ESCO.

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

II. Privacy and Data Security

(1) Data and/or Confidential Utility Information will at all times remain the sole property of the Party collecting the ~~d~~Data and/or Confidential Utility 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 ~~C~~confidential ~~i~~information of the other Party.

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

(3) ESCO must provide 20 business days prior written notice to Utility if a new Third Party Representative will be engaged by ESCO to support the data exchange with Utility. ESCO will assist Utility in providing information, in form and substance reasonably sufficient to Utility, regarding the state of the internal control environment of the Third Party Representative to enable Utility to perform ~~any~~ a reasonable 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 reasonable requirements, provided that such requirements shall not be any more restrictive than those set forth in the Addendum.

Comment [pl34]: 20 days may be overly burdensome in certain instances.

(4) ESCO 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~~ reasonable discretion, whether or not the obligations and terms are sufficient.

(5) At any and all times during which ESCO or Third Party Representative is engaged in ~~data~~ the exchange of Confidential Utility Information with Utility, ESCO and its Third Party Representative(s) will:

i. Have ~~appropriate and~~ reasonable security controls and/or measures in place to protect and safeguard the Confidential Utility Information ~~data exchange with Utility~~ from disclosure or unauthorized access and/or use. ESCO 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~~standards 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~~Confidential Utility Information according to industry recognized ~~best practices~~standards 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 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 to be applicable to Utility~~.

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

v. Safely secure or encrypt ~~data~~ Confidential Utility Information during storage or transmission.
~~Store data only within the boundaries of the United States.~~

vi. Except as may be necessary in connection with the ~~data~~ exchange of Confidential Utility Information, not store ~~data~~ Confidential Utility Information on removable devices or media.
~~Not back up data to the cloud without Utility's prior written approval.~~

(6) If ESCO uses a service provider or co-location data center, ESCO 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 of Confidential Utility Information includes the use of ESCO'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.centralhudson.com/privacy/index.aspx.

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

i. ESCO 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 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 and its Third party Representative(s) agrees that, in the event of a Cyber Incident arising out of or relating to ESCO or Third Party Representative's premises or equipment contained thereon, ESCO and Third Party Representative(s) shall provide ~~full~~ reasonable 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'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 and its Third Party ~~Representaitive~~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 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 exchanges ~~d~~Data with Utility, ESCO 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.~~i. ~~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.~~ii. 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 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.~~iii. Upon Utility's request, ESCO and each Third Party ~~Represetnative~~Representative shall promptly provide the results of any vulnerability assessment and penetration test.

~~vi.~~iv. 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.

Comment [pl35]: Obligations under II(5) should be sufficient.

~~vii.~~v. Upon Utility's request, ESCO 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 required security activities have been performed, and all identified security issues have been documented and resolved.

(2) ESCO warrants that, to its knowledge, the application system contains no virus, Trojan, worm, undocumented shutdown mechanism or other code or feature which is intended, or is known by ESCO as likely, to disable, damage, destroy, deny access to or degrade the performance of the application system, or Confidential Utility Information, Data or other information technology resource. ESCO warrants that, to its knowledge, the application system contains no backdoors or other feature that is intended to allow ESCO or someone else to gain unauthorized or surreptitious access to the application system or Data or other information technology resources. ESCO 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)~~(1) ESCO shall remain responsible for any Cyber Event or Cyber Incident in relation to its or its Third Party ~~Represnetatives~~Representatives' obligation set forth in the Addendum and Data Security Rider.

~~(3)~~(2) ESCO and their Third Party Representative(s) shall notify Utility of a ~~c~~Cyber~~-~~ ~~i~~Incident based on the ~~Notification Table~~notification obligations set forth in the Addendum. ~~Upon Utility's request, ESCO shall utilize and pay the cost for a computer forensic expert to investigate the incident that is either provided by ESCO 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~~

Comment [pl36]: ESCO is not a software as a service provider. There are no uptime guarantees. These reporting obligations conflict with the reporting obligations in the Addendum. The inclusion of this chart is unreasonable.

~~(4)~~(3) ESCO and its Third Party Representative(s) shall establish policies and procedures to properly investigate a Cyber Event or Cyber Incident caused by ESCO or its Third Party Representative and be willing to work with Utility's forensic examiner.

~~(5)~~(4) Notification will be made to the main contact at Utility and to cybersecurity@cenhud.com.

V. Right to Audit

(1) Upon Utility's request, ESCO shall provide reasonable evidence that the controls of ESCO and its Third Party Representative(s) include the proper security controls in place to protect Utility's ~~data~~ Confidential Utility Information and to ensure that ESCO's Third ~~p~~Party Representatives' information systems related to the data exchange are operating effectively to ensure availability. The evidence may include, as reasonably determined by Utility, ESCO 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 verifying that ~~that~~ ESCO and its Third ~~p~~Party Representative(s) are in compliance~~, such as an ISO 27001 or PCI DSS certification letter~~.

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

Comment [pl37]: This provision conflicts with the Audit provisions in the Addendum and in the Attestation. There should not be three separate audit provisions.

Comment [pl38]: This is unreasonable.

EXHIBIT B

THIRD-PARTY REPRESENTATIVE ADDENDUM

I, _____, have read the Addendum between _____, ("Company") and Central Hudson Gas & Electric 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 Utility Information disclosed by Utility to the ESCO pursuant to the Addendum.

Comment [pl39]: This should be ESCO to match Addendum definition.

Comment [pl40]: It does not make sense for Third Party Representatives to have to comply with every obligation placed upon ESCO. Those specific provisions that need to be flowed down should be called out in the Addendum.

_____ _____

Signature Date

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

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").

Comment [pl41]: Defined terms should match the Addendum. This would be ESCO in this form of the Addendum.

WHEREAS, Third Party desires to retain access to certain Confidential Utility Information (as defined previously in this ~~Data Security Agreement~~Addendum), 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, unless otherwise required or prevented by law, 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~~in accordance with the terms of the Addendum.

_____ Role-based access controls are used to restrict system access to authorized users and limited ~~on a need to know basis~~based on job function or other legitimate business reason.

_____ 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, unless there is a reasonable basis not to do so. 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, unless

_____ impracticable.

_____ 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 if they contain Confidential Utility Information.

~~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,~~ solely 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

Comment [pl42]: Audit scope needs to be defined and coordinated between provisions of the Addendum. There should not be three audit provisions.

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:

DATA SECURITY AGREEMENT

The Brooklyn Union Gas Company

d/b/a

National Grid

And

_____

Name (Print)

Version 5-9-2018

THIS DATA SECURITY AGREEMENT, including Exhibits attached hereto and made a part hereof (this "Agreement") which are incorporated by reference herein, is made as of this _____ day of _____ , 20___ (the "Effective Date") by and between National Grid operating companies: The Brooklyn Union Gas Company d/b/a National Grid NY, with offices at 175 East Old Country Road, Hicksville, NY 11801 (collectively "National Grid" or "Utility") and _____, an ESCO, DER, or EDI Vendor (hereinafter referred to as "Third Party") with offices at _____; and together with Utility the ("Parties" and each, individually, a "Party"). In the event a Business Services Agreement ("BSA") exists between the Parties, this Agreement shall be incorporated by reference into the terms of the BSA.

RECITALS

WHEREAS, Third Party 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 Third Party aggregated customer information; and

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

WHERAS, Utility and Third Party also desire to enter into this Agreement to establish, among other things, the full scope of Third Party'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, collectively, aggregated and customer-specific information that Utility is: (A) required by the Commission to provide to Third Party and (B) any other Utility-specific, aggregated, Personal Data, Sensitive Data, or Utility Data, or customer-specific data provided to Third Party by Utility. Confidential Utility Information shall not include any information of Third Party which: (A) was in the public domain at the time of disclosure by Utility to Third Party; (B) became part of the public domain after disclosure by Utility to Third Party through no fault of Third Party; (C) was acquired by Third Party independently after disclosure by Utility to Third Party, from a third party without breach of agreement or violation of law; or (D) was in Third Party's possession prior to the time of disclosure by Utility to Third Party. For avoidance of doubt, data collected by Third Party from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with Third Party or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Agreement.

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 Third Party or its Representative's Processing of Confidential Utility Information; (B) the Utility's internal requirements and procedures that are provided by Utility to Third Party relating to the protection of information that identifies or can be used to identify an individual that apply with respect to Third Party 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 Third Party 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; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by Third Party or any current or former Representatives. Good faith acquisition of Confidential Utility Information by an employee or agent of Third Party for the purposes of the business is not a Data Security Incident, provided that the Confidential Utility Information is not misused or subject to unauthorized disclosure.

Comment [pl1]: An inadvertent corruption of data could be a normal business event fixed through routine backup procedures. This should not be deemed a Data Security Incident.

Comment [pl2]: Same comment as above

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, except as otherwise required by law, including but not limited to record retention requirements and litigation holds .

e. "Third Party" 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; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial, or health information; or (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.

Comment [pl3]: This definition is overly broad. At a minimum, this should be limited to first and last name and address in combination with one of (C) through (H). E.g. a zip code, by itself, should not be considered Personal Data.

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, including Social Security number, passport number, driver's license number, Utility customer account number, Municipal Identification (NYCID), or similar identifier.

j. "Third-Party Representatives" or "Representatives" mean those agents of Third Party that are Electronic Data Interchange vendors, contractors or subcontractors.

k. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of Third Party or a third party and whether or not it is provided to Third Party.

2. **Scope of the Agreement.** This Agreement shall govern and apply as of the Effective Date to all Confidential Utility Information disclosed to Third Party by Utility or to which Third Party is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by Third Party (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 customer financial account information will be provided pursuant to this Agreement. If any information is inadvertently sent to Third Party, Third Party will ~~immediately~~ promptly notify the Utility and Destroy any such information in the appropriate manner. Third Party, and its Third Party Representatives, shall have a grace period of twelve (12) months from the Effective Date of this Agreement in which to cure any deficiencies with respect to its obligations under this Agreement, provided that Third Party and its Third Party Representatives work diligently and in good faith to come into compliance during such grace period.

3. **Third Party Compliance with all Applicable Commission Uniform Business Practices.**

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

_____Third Party 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.

_____Third Party is a vendor, agent or other entity providing services to an ESCO or DER.

Comment [pl4]: Should be limited to EDI vendors, or those that have access to Utility's systems. Cloud storage providers (e.g. Amazon Web Services) are not going to agree to these terms or sign any Representative Addendum.

Application of the terms in this Agreement should vary based on the specifics of the application by the Third Party Representative. For example, EDI providers have different access and risk than marketing contractors and/or brokers. One size does - and should not - fit all.

Comment [pl5]: This conflicts with the definition of Confidential Utility Information provided above and unnecessarily expands the scope to information that is beyond that sought to be protected and so is therefore unreasonable.

Comment [pl6]: Companies that fall under this category are presumably Third Party Representatives to ESCOs. As such why would such entities have to BOTH execute a DSA and a Third Party Representative Agreement? These provisions are circular.

4. **Customer Consent.** Third Party warrants that it has obtained informed consent from all customers about whom Third Party requests ~~data~~ Confidential Utility Information and that it will retain such consent for a period of at least six years. Third Party agrees to provide proof of customer consent at the request of Utility and Utility reserves its right to audit Third Party for compliance with consent requirements herein. Third Party agrees that upon a customer revocation of consent, Third Party warrants that it will no longer access said customer's Confidential Utility ~~i~~Information and that it will Destroy any of said customer's Confidential Utility ~~i~~Information in its or its Representative's possession.

5. **Provision of Information.** Utility agrees to provide to Third Party or its Representatives, certain Confidential Utility Information, as requested, provided that (A) Third Party and its Representatives are in compliance with the terms of this Agreement; (B) if required by Utility, Third Party has provided and has caused its Representatives to provide, ~~-~~to ~~-~~the satisfaction of Utility ~~any~~ the Vendor Product/Service Security Assessment~~s,~~ attached hereto as Exhibit A or such other risk assessment forms as Utility may reasonably require from time to time, but not more than once per year ("Assessment") and Third Party will comply with the Utility Assessment requirements as negotiated by the Parties; (C) Third Party (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as detailed in the Assessment and reasonably acceptable to Utility to protect Confidential Utility Information; and (D) Third Party complies and shall cause its Third-Party Representatives to comply with ~~Utility's data protection programs~~ the agreed-upon Assessment requirements. Provided the foregoing prerequisites have been satisfied, Third Party shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to Third Party.

6. **Confidentiality.** Third Party shall: (A) hold all Confidential Utility Information in strict confidence; except as otherwise expressly permitted by Section 7 ~~-~~herein; (B) ~~-~~not disclose Confidential Utility Information to any other person or entity (including but not limited to subcontractors, affiliates, or members of Third Party); ~~(C) not Process Confidential Utility Information outside of the United States;~~ (~~D~~C) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Agreement; (~~E~~D) limit reproduction of Confidential Utility Information; (~~F~~E) 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~~F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as Third Party 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~~G) to the extent required by the Utility, each ~~person with a need to know the Confidential Information~~Representative shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, Utility shall have the right to request ~~further~~ reasonable assurances that the foregoing restrictions and protections concerning Confidential Utility Information ~~-~~are being observed and Third Party shall be obligated to promptly provide Utility with the requested assurances. Data and/or ~~C~~confidential ~~I~~information will at all times remain the sole property of the Party collecting the data and/or ~~C~~confidential ~~I~~information. Nothing

Comment [pl7]: This sentence suggests that ESCOs cannot hold CUI. Was this sentence meant to say something else? For example, what is the notice mechanism?

Comment [pl8]: It is not clear which specific provisions flow down to Third Party Representatives.

Comment [pl9]: Exhibit A refers to an "Individual Non-disclosure Agreement". Is this meant to refer to the "Self-Attestation of Information Security Controls"?

Comment [pl10]: Please define these or remove.

Comment [pl11]: Should be mutual, covering ESCO information flowing back to Utility.

Comment [pl12]: Services are not defined in the Recitals.

Comment [pl13]: Is this being required?

Comment [pl14]: Individual employees should not be required to sign anything.

Comment [pl15]: There is no Exhibit B. Is this meant to refer to Exhibit A?

Comment [pl16]: Terms are not defined.

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 ~~D~~data and/or ~~C~~confidential ~~I~~information of the other Party.

Comment [pl17]: Terms are not defined.

7. Exceptions Allowing Third Party to Disclose Confidential Utility Information.

a. Disclosure to Representatives. Notwithstanding the provisions of Section 6 herein, Third Party may disclose Confidential Utility Information to its ~~contractors or subcontractors~~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 Representative ~~first~~ (A) is advised by Third Party of the sensitive and confidential nature of such Confidential Utility Information; ~~-~~(B) agrees to comply with the provisions of this Agreement~~, provided that with respect to Representatives and this subsection (B), such Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Representatives were Third Party~~; and (C) signs the Representative Agreement. ~~All such written agreements with Representatives shall include direct liability for the Representatives towards Utility for breach thereof by the Representatives, and a copy of such agreement and each~~ The Representative Agreement ~~and Third Party agreement~~ shall be made available to Utility upon request. ~~Notwithstanding the foregoing, Third Party shall be liable to Utility for any act or omission of a Representative, including without limitation, Representatives that would constitute a breach of this Agreement if committed by Third Party.~~

Comment [pl18]: Not defined.

Comment [pl19]: Is this meant to refer to current Exhibit A - Individual Non-Disclosure Agreement? Exhibit references need to be sorted out.

Comment [pl20]: Individual employees should not be required to sign anything. If required, it should apply to Third Party Representatives.

b. Disclosure if Legally Compelled. Notwithstanding anything herein, in the event that Third Party or any of its 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), Third Party shall, except to the extent prohibited by law, ~~within 24 hours~~promptly notify Utility, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, Utility shall have the right to consult with Third Party 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, Third Party and its 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 Third Party and its 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**. Within ~~ten~~ thirty (~~10~~30) days after Utility's written demand based upon a good faith business reason, Third Party shall (and shall cause its Representatives to) take reasonable steps 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~~,~~ and format that the Confidential Utility Information was provided to Third Party, and in such 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 Third Party's or its Representatives' possession as a result of the Utility and as set forth herein, including destroying ~~-~~Confidential Utility Information from all systems, records, archives, and backups of Third Party and its Representatives, and all subsequent ~~access, use, and~~ Processing of the Confidential Utility Information by Third Party and its Representatives shall cease. Notwithstanding the foregoing, Third Party and its 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, or as required by law, provided that Third Party and its Representatives shall ~~(1) not have experienced a Data Security Incident,~~ (~~2~~1) not permit access to or recovery of Confidential Utility Information from such computer backup system and (~~3~~2) keep all such Confidential Utility Information confidential in accordance with this Agreement. Third Party shall, upon request, certify to Utility that the destruction by Third Party and its Representatives required by this Section has occurred by (A) having a duly authorized officer of Third Party complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Representatives and maintaining them on file. Compliance with this Section 8 shall not relieve Third Party from compliance with the other provisions of this Agreement. The obligations under this Section shall survive any expiration of termination of this Agreement.

9. **Audit.** Upon reasonable notice to Third Party, Third Party shall, and shall require its Representatives to permit Utility~~, its~~ auditors~~,~~ or designated audit representatives~~, and regulators~~ to audit and inspect, at Utility's sole expense ~~(except as otherwise provided in this Agreement)~~, and no more often than once per year (unless otherwise required by Utility's regulators): (A) the facilities of Third Party and Third Party's Representatives where Confidential Utility Information is Processed by or on behalf of Third Party; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) Third Party'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~~, at a minimum,~~ solely for the purpose of verifying Third Party's compliance with this Agreement, including all applicable Data Protection Requirements. Notwithstanding the generality of the foregoing, the audited party shall not be required to provide access to records to the extent that such access is prohibited by applicable law or if such records are legally privileged or outside the scope of verifying compliance with this Agreement. In addition, and notwithstanding the foregoing or anything else in this Agreement, the audit must be conducted pursuant to the parameters of the audited party's own policies, standards, and procedures for information security risk assessments. Notwithstanding anything herein, in the event of a

Comment [pl21]: 10 days is unreasonable, especially when accounting for (potentially) multiple layers of Representatives.

Comment [pl22]: Utility can ask ESCO to delete data at any time without reason, effectively shutting the ESCO down? This is unreasonable. There needs to be a legitimate reason for Utility to request the return or destruction of information.

Comment [pl23]: A minor Data Security Incident (e.g. inadvertent corruption of data) would preclude the allowance of backups? This is unreasonable.

Comment [pl24]: This is unreasonable, especially considering how broadly Third Party Representatives is defined. Certain vendors may not be agreeable to this. Vendors may object to being subjected to an audit by parties that they are not in contract with.

Comment [pl25]: What data security provisions are in place for these auditors to protect and secure information obtained about ESCO data, systems, security, etc. What insurance is in place? Will ESCOs be additional insureds? Where will the information be stored? How secured?

Comment [pl26]: Needs to be defined further (see comment to definition).

Data Security Incident, Third Party shall and shall cause its Representatives to permit an audit hereunder more frequently than once per year, as may be reasonably requested by Utility. Third Party shall ~~immediately~~ promptly correct any deficiencies reasonably identified by Utility.

10. Investigation. Upon reasonable notice to Third Party, Third Party shall assist and support Utility where reasonable in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to a Data Security Incident involving Confidential Utility Information Processed by Third Party on behalf of Utility, and without waiver by ESCO of any rights or privileges under applicable law. Such assistance shall be at Utility's sole expense, except where such investigation was required solely due to the proven acts or omissions of Third Party or its Representatives, in which case such assistance shall be at Third Party's sole expense.

11. Data Security Incidents. Third Party is responsible for any and all Data Security Incidents caused by Third Party or its Representatives involving Confidential Utility Information that is Processed by~~, or on behalf of,~~ Third Party or its Representatives. Third Party shall, except as otherwise required by law, promptly notify Utility in writing ~~immediately~~ (and in any event within ~~twenty-four (24) hours~~five (5) business days) whenever Third Party reasonably believes that there has been a Data Security Incident. The notification required by this Section 11 may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation, and such notification shall only be made after such law enforcement agency determines that such notification does not compromise such investigation. After providing such notice, Third Party will investigate the Data Security Incident, and ~~immediately~~ promptly take ~~all necessary~~reasonable 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~~. Third Party further agrees to provide, at Third Party'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, Third Party shall not notify any individual ~~or any third party~~ other than law enforcement or third parties protected under attorney-client privilege of any ~~potential~~ Data Security Incident involving Confidential Utility Information without first ~~consulting with~~ disclosing to, and obtaining the permission of, Utility, such permission not to be unreasonably withheld, conditioned or delayed. In addition, within 30 days of ~~identifying or being informed~~notification to Utility of a Data Security Incident, Third Party shall develop and execute a plan, those unprivileged or protected portions subject to Utility's reasonable approval, that reduces the likelihood of a recurrence of such Data Security Incident. Third Party agrees that Utility may at its reasonable discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a subsequent Data Security Incident occurs.

12. **Cybersecurity Insurance Required.** Third Party shall carry and maintain ~~C~~cybersecurity insurance in an amount of no less than ~~ten~~ two million five hundred thousand dollars ($~~1~~2~~0~~,~~0~~500,000) per incident and Utility shall be included by endorsement as an additional insured on Third Party's ~~C~~cybersecurity insurance. Third Party agrees to cause its ~~Contractors~~ Representatives to carry and maintain cybersecurity insurance in the amount shown above.

13. **No Intellectual Property Rights Granted.** Except as otherwise set forth herein or agreed to in writing by the Parties, ~~N~~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 Third Party shall acquire no ownership interest in the Confidential Utility Information (which, as between Third Party 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 Agreement.

14. **Additional Obligations.**

a. Third Party shall not create or maintain data which are derivative of Confidential Utility Information except for a legitimate business purpose, such as for the purpose of performing its obligations under this Agreement or as authorized by Utility. ~~Data collected by Third Party from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with Third Party or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Agreement.~~

b. Third Party 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 Third Party to be applicable to Utility~~.

c. Third Party 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 Third Party's internal use, Processing, or other transmission of Confidential Utility Information, whether between or among Third Party's Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of Third Party, including without limitation Representatives.

d. Third Party shall ~~safely~~ reasonably secure or encrypt all Confidential Utility Information during storage or transmission.

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

Comment [pl27]: Utility should make a tariff amendment before it can require insurance in an amount that will directly impact customer pricing. Such a requirement may result in "unreasonable or burdensome" costs. Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25; *See also* Case 96-E-0909, Matter of Central Hudson Gas & Electric Corporation's Plans for Electric Rate/Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 22.

Comment [pl28]: $10M is not industry standard for this type of data.

Comment [pl29]: It is unreasonable to flow this down to all Third Party Representatives, considering how broadly this is defined. This is also unnecessarily redundant. There will be different levels of Third Party Representatives with different levels of access. Terms flowed down should vary. An EDI vendor is different than a marketing vendor/broker with limited access to CUI.

Comment [pl30]: Moved to definition section.

Comment [pl31]: Needs to be defined further (see comment to definition).

f. Third Party 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~~ has an interest in the ~~Confidential Utility Information, data~~ theft~~,~~ or other unauthorized release, disclosure or misuse 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 Third Party's ~~accessing or~~ Processing of such Confidential Utility Information.

15. **Payment.** In consideration of Utility's agreement to provide Confidential Utility Information in accordance with Section 2, Third Party shall pay to Utility fees pursuant to its tariffs.

16. **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 the provision or Processing of Confidential Utility Information hereunder. Third Party 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 and Limitation of Liability.** To the fullest extent permitted by law, ~~Third Party~~each Party shall indemnify and hold ~~Utility~~the other Party, 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 ~~Third Party or any of its Representatives~~such Party. Notwithstanding anything to the contrary, in no event shall any Party be liable for or entitled to indirect, special, punitive, (including but not limited to any loss for anticipated revenue, earnings or profits, lost opportunity or increased expense or operations) or consequential damages whether by statute, in contract, or tort pursuant to or in connection with this Addendum and all such damages are hereby expressly disclaimed and waived.

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.

Comment [pl32]: To the extent Utility shares any liability that may be gross negligence or willful misconduct, the limitation may be prohibited under 16 NYCRR 218.1. *See also* Case 96-E-0891 - Matter of New York State Electric & Gas Corporation's Rate/Restructuring Pursuant to Opinion No. 96-12. Retail Access Tariff Filing, Order Concerning Tariff Amendments to Establish a Retail Access Program (issued Apr. 29, 1998), at 25.

Comment [pl33]: The miscellaneous provisions should correspond any existing agreement with National Grid.

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 Third Party, to:

Third Party Name:
Name of Contact:
Address:
Phone:
Email:

If to Utility, to:

National Grid
Customer Choice Department
175 East Old Country Road
Hicksville, NY 11801
Att: KEDNY DSA

With a copy to:
National Grid Legal Department
NY Regulatory Group
300 Erie Blvd West
Syracuse, NY 13202

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 Agreement shall be effective as of the date first set forth above and shall remain in effect ~~until~~ unless terminated by Utility or Third Party ~~upon not less than 10 days' prior written notice specifying the effective date of termination,~~for material breach by the other Party; 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~~; and provided, further, that Utility may terminate this Agreement immediately upon notice to Third Party in the event of a material breach hereof by Third Party or its 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 Third Party nor its Representatives shall have any further right to Process Confidential Utility Information and shall ~~immediately~~ promptly comply with its obligations under Section 8.

Comment [pl34]: The term should run concurrent with any existing National Grid contract.

Comment [pl35]: Section references are not consistent across all DSAs.

20. Consent to Jurisdiction; Selection of Forum. ~~Third Party~~The Parties irrevocably submit~~s~~ 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 Agreement. ~~Third Party~~The Parties agree~~s~~ that service of process on ~~it~~ a Party in relation to such jurisdiction may be made by certified or registered mail addressed to ~~Third Party~~the served Party at the address for ~~Third Party~~such Party pursuant to Section ~~11~~ 18 hereof~~.~~, which will be effective upon actual receipt by served Party ~~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~~. ~~Third Party~~Parties agree~~s~~ that service of process ~~on it~~ may also be made in any manner permitted by law. ~~Third Party~~Parties consent~~s~~ to the selection of the New York State and United States courts within New York or Kings County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement, unless otherwise required by law. Nothing in this Section 20 shall diminish or circumvent the dispute resolution rights and obligations, or the procedure for dispute resolution pursuant to Section 33 of this Agreement.

21. 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.

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

23. 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.

24. Amendments; Waivers. 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.

25. Assignment. This Agreement ~~(and Aggregator's obligations hereunder)~~ may not be assigned by ~~Third Party or Representatives~~either Party without the prior written consent of ~~Utility~~the other Party, and any purported assignment without such consent shall be void. Such consent shall not be unreasonably withheld, conditioned or delayed.

26. 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.

27. **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.

28. **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.

29. **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 other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, ~~or~~ communications failure or governmental action or order) 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.

30. **Relationship of the Parties.** Utility and Third Party 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.

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

32. **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.

~~32.~~33. **Dispute Resolution**. Each Party shall use its best efforts to resolve any dispute related to this Agreement between them promptly and amicably and without resort to any legal process if feasible within thirty (30) days of receipt of a written notice by one Party to the other Party of the existence of such dispute. The dispute resolution process in Section 8 of the Uniform Business Practices ("UBP") is incorporated as if set forth fully herein. In addition to UBP Section 8, Third Party may also seek relief from the Public Service Commission pursuant to its reserved authority over Utility-ESCO operating agreements for purposes of dispute resolution. 98-E-0952 - Matter of Competitive Opportunities Regarding Electric Service, Statement of Regulatory Policies Regarding Operating Agreements (issued Mar. 10, 1998).

Comment [pl36]: *See also* 96-E-0909 - Matter of Central Hudson Gas & Electric Corporation's Plans for Electric/Rate Restructuring Pursuant to Opinion 96-12, Order Concerning Tariff Amendments that Include Provisions to Implement a Retail Access Program for Central Hudson Gas & Electric Corporation (issued June 30, 1998), at 21 & n.1 (citing to Statement of Regulatory Policy, and referencing previously reserved authority to resolve disputes for both operating agreements and handbooks).

[signature page follows]

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

The Brooklyn Union Gas Company d/b/a National Grid	**Third Party**
Signature: _____	Signature: _____
Name: Terrence Kain	Name (Print): _____
Title: Director, Customer Choice	Title: _____
Date:_____	Date:_____

Exhibit A

INDIVIDUAL NON-DISCLOSURE AGREEMENT

Comment [pl37]: Make uniform with other DSAs to the extent possible. Some utilities are not requiring this form (Con Ed).

I, (print) _____ , have read the Agreement between (print)_____, ("Third Party") and National Grid, ("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 Utility Information disclosed by Utility to Third Party pursuant to the Agreement.

Signature: _____

Date: _____

SELF-ATTESTATION

OF INFORMATION SECURITY CONTROLS

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, unless otherwise required or prevented by law, 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~~in accordance with the terms of the Addendum.

_____ Role-based access controls are used to restrict system access to authorized users and limited ~~on a need-to-know basis~~based on job function or other legitimate business reason.

_____ 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, unless there is a reasonable basis not to do so. 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, unless impracticable.

_____ 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 if they contain Confidential Utility Information.

~~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,~~ solely 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.

Comment [pl38]: Audit scope needs to be defined and coordinated between provisions of the Agreement. There should not be three audit provisions..

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

Signature: _____

Name: _____

Title: _____

Date: _____