April 29, 2019

Via electronic mail

Hon. Kathleen H. Burgess
Secretary to the Commission
New York State Public Service Commission
Empire State Plaza
Agency Building 3
Albany, NY 12223-1350
secretary@dps.ny.gov

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

Please find enclosed the Response of Mission:data Coalition to the Commission's Notice Soliciting Comments dated February 20, 2019. The aforementioned notice also cited Case Nos. 18-M-0084, 16-M-0411 and 15-M-0180.

If you have any questions about this letter or have difficulty viewing the enclosed PDF, please contact me

Respectfully submitted,

Michael Murray, President
Mission:data Coalition
1752 NW Market St #1513
Seattle, WA 98107
(510) 910-2281 (phone)
michael@missiondata.io

STATE OF NEW YORK

PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	Case 18-M-0376
In the Matter of a Comprehensive Energy Efficiency Initiative	Case 18-M-0084
In the Matter of Distributed System Implementation Plans	Case 16-M-0411
In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products	Case 15-M-0180

Response of Mission:data Coalition

To the Commission's February 20, 2019 Notice Soliciting Comments

1. Introduction

On February 20, 2019, the New York Public Service Commission ("Commission") issued the above-referenced Notice Soliciting Comments (the "Notice"), in which the Commission asked for comments from parties regarding several petitions, described below. Mission:data Coalition ("Mission:data") hereby submits this Response to the Notice.

Mission:data strongly urges the Commission to dismiss the February 4, 2019 Joint Utilities' *Petition for Approval of the Business-to-Business Process Used to Formulate a Data Security Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement by Entities Seeking Access to the Utility Customer Data or Utility Systems* in Case Nos. 18-M-0376 and 15-M-0180 (the "Joint Utility Petition"). While a well-known cybersecurity breach occurred in 2018 at a vendor to energy services

companies ("ESCOs"), the Joint Utilities seek to exploit the current climate of fear surrounding cybersecurity risks in order to inappropriately seize certain powers over distributed energy resource ("DER") suppliers. Such powers are exceptionally broad in scope and would be in conflict with prior Commission orders. Furthermore, by granting the Joint Utility Petition, the Commission would abdicate its authority on policymaking and dispute resolution, and would delegate such authorities exclusively to the utilities without justification. Finally, given the chilling effect on DERs that approval of the Joint Utilities Petition would have, Mission:data concludes that, if approved, the Commission must necessarily retract substantial portions of the "Reforming the Energy Vision" ("REV") policy framework as they relate to third-party DERs. Finally, to resolve the disputes surrounding Data Security Agreements more holistically, Mission:data recommends using Staff's distinction between "system risk" and "data misuse risk" to require utilities to own their system risk, but the Commission should explicitly waive the Joint Utilities' liability for data misuse risk so long as the data is transferred pursuant to customer consent and is encrypted in transit.

2. Background

On November 21, 2017, Mission:data filed a *Petition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements* ("Mission:data Petition") in which Mission:data sought interpretation of the October 19, 2017 *Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers* ("DER Oversight Order").

On November 8, 2018, the JU submitted a *Petition for Declaratory Ruling Regarding Their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices* ("JU Declaratory Ruling Petition").

On February 4, 2019 in Case Nos. 18-M-0376 and 15-M-0180, the Joint Utilities[1] filed a *Petition for Approval of the Business-to-Business Process Used to Formulate a Data Security*

[1] The Joint Utilities (or "JU") consist of Consolidated Edison Company of New York, Inc. ("ConEd"), 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, and New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation.

Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement by Entities Seeking Access to the Utility Customer Data or Utility Systems (the "Joint Utility Petition").

3. The Joint Utility Petition Seeks Authorities That Are Inconsistent Or Incompatible With Commission Orders

The Joint Utility Petition seeks exceptionally broad authority that goes well beyond what the Commission has dictated in previous orders. The Joint Utility Petition would, if approved, be incompatible with Commission orders in at least six (6) different respects. Each of the reasons represent a fatal flaw to the Joint Utilities Petition.

a) The Joint Utilities seek to enforce Data Security Agreements on all entities, but the DER Oversight Order states that data security agreements do not apply to DERs that use Green Button Connect ("GBC").

First, as we argued in the Mission:data Petition,[2] the DER Oversight Order clearly states: "This section does not impose any obligations on DER suppliers that do not request or receive data using EDI [Electronic Data Interchange]." The section in question, Section 2(C), refers in sub-section (F) to the NIST Cybersecurity Framework ("DER suppliers that obtain customer information from the distribution utility or DSP must have processes and procedures in place regarding cybersecurity consistent with the National Institute of Standards and Technology Cybersecurity Framework") and in sub-section (G) to data security ("DER suppliers that obtain customer information from the distribution utility or DSP must comply with any data security requirements imposed by that utility or by Commission rules on ESCOs and/or any data security requirements associated with EDI eligibility"). Such provisions are clearly exempted for DERs that use GBC, and yet the Joint Utilities Petition would, if granted, violate the plain language of the DER Oversight Order.

[2] Mission:data Coalition. Petition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements. Case No. 18-M-0376, dated November 30, 2018.

b) The Joint Utilities seek the authority to terminate data access to DERs that use GBC, but the Uniform Business Practices – Distributed Energy Resource Suppliers ("UBP-DERS") have no such provision.

In the "final" version of the Data Security Agreement and Self-Attestation of Information Security Controls ("DSA") dated August 16, 2018 and posted on the Commission's website,[3] the DSA allows the utility to unilaterally terminate data-sharing with a DER:

> This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated in accordance with the provisions of the service agreement, if any, between the Parties or the UBP or UBP DERS and upon not less than thirty (30) days' prior written notice...**Further, Utility may terminate this Agreement immediately upon notice to ESE in the event of a material breach hereof by ESE or its Third-Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 14, 16, and 24 shall be a material breach hereof**...[4]

The entity that decides whether a DER is in breach of the DSA is not specified. In the absence of a neutral, independent party making such a determination (such as the Commission), the Joint Utilities will undoubtedly seize on the opportunity to revoke electronic access at the sole discretion of the Joint Utilities without needing to satisfy an objectively-determined, independently-verified violation of the DSA. Mission:data believes that the language above, in particular its lack of due process before the Commission surrounding a potential DSA violation, would in effect grant utilities the right of unilateral termination. After all, the determination of whether a violation occurred would be in the utilities' hands. (Furthermore, as explained below, DERs that use Green Button Connect ("GBC") will immediately be in breach of the DSA after commencing electronic communications via GBC, so termination by the Joint Utilities is a constant threat even in the absence of the DER causing harm to the customer or utility.)

---

[3] The DSA and related materials are posted at http://www3.dps.ny.gov/W/PSCWeb.nsf/All/4A24D0D51395B1F8852582A2004398A3?OpenDocument.

[4] Data Security Agreement at p. 12. Emphasis added. http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/4a24d0d51395b1f8852582a2004398a3/$FILE/86804390.pdf/DSA%20Final%20Clean%2008-16-2018.pdf

However, there is no termination right of the Joint Utilities specified in the UBP-DERS. The only mention of the word "termination" in the UBP-DERS is in relation to termination fees that DERs charge customers.[5] It would appear that the Joint Utilities have presumed that they can avail themselves of termination provisions approved only for ESCOs and apply such termination provisions to DERs without authorization by the Commission. Section 2(F)(1)(a) of the UBP-ESCO is cited by the Joint Utilities[6] as the source of their authority to terminate access to DERs that use GBC, but the UBP-ESCO do not apply to DERs. The truth is that the Commission-approved UBP-DERS provide no such termination right by the Joint Utilities. Simply put, the Joint Utilities claim an authority over DERs that does not exist.[7]

c) The DSAs originated from a Commission order that did not include DERs in the definition of "energy services entities."

On June 14, 2018, the Commission issued an *Order Instituting Proceeding* in Case No. 18-M-0376, thereby beginning the process that led to the development of the DSA. Once again, the Joint Utilities assert an equivalence between users of the EDI and GBC platforms that does not exist in the plain text of Commission orders. Case No. 18-M-0376's *Order Instituting Proceeding* defined energy services entities ("ESEs") as "ESCOs, Electronic Data Interchange (EDI) providers, and any other third party that contracts with an ESCO to communicate data between the ESCO and the utility."[8] Of course, DER providers often seek access to customer data (with customer permission) without being a commodity supplier or without contracting with an ESCO.

This is not the first time the Joint Utilities have asserted that there should be equivalent treatment between entities that use EDI and GBC despite Commission orders stating otherwise. In a *Request for Clarification* dated November 21, 2018, the Joint Utilities argue that the

---

[5] See, e.g., Section 3(C)(B)(2)(A)(2) of UBP-DERS.

[6] Joint Utilities Petition at p. 16.

[7] The Joint Utilities have acknowledged that existing Commission orders and rules do not provide the Joint Utilities with explicit termination rights, an authority the Joint Utilities seek from the Commission: "The Joint Utilities *assert* that the following DERS UBP rule applies to all DERS, regardless of the platform they are using to obtain customer-specified data..." Joint Utilities Petition at p. 16. Emphasis added.

[8] Case No. 18-M-0376, Order Instituting Proceeding. June 14, 2018 at p. 2.

Commission should amend the DER Oversight Order so that DERs that use GBC become subject to Section 2C's provisions in order to "provide essential protections to customers and Commission oversight over DERS."[9] However, the Joint Utilities simultaneously admitted that the UBP-DERS as written does not apply to entities that use EDI: "Section 2C, however, applies only to DERS obtaining data through EDI, and specifically does not apply to other either existing or planned platforms for receiving customer data."[10] Twice the Commission has limited the application of data security provisions to entities that use EDI, and yet the Joint Utilities Petition ignores this important distinction.

d) Granting Joint Utilities the power to amend the DSA in unknown ways in the future would likely lead to conflicts with Commission orders and rules.

The Joint Utilities seek not only the power to enforce the DSA as they see fit but also the unilateral authority to modify the DSA in unknown and unknowable ways in the future. The Joint Utilities ask the Commission to:

> Authorize the amendment of the DSA going forward through the business to business process which should include at a minimum, standard requirements that: (1) specify compliance with the Uniform Business Practices ("UBP"), UBP DERS, or other applicable Commission rules; (2) address the transfer of information; (3) maintain the confidentiality of Joint Utilities and the ESCOs, DERS, Direct Customers, and their applicable contractors (collectively, "Energy Service Entities" or "ESEs") information, including the protection of customer data; (4) requiring the return and destruction of information; (5) address each Party's responsibility and liability for data security incidents; (6) require cyber security insurance; (7) define minimum cyber security requirements; (8) address how to determine whether ESEs have and maintain minimum levels of cyber security; and (9) require ESE indemnification of the Joint Utilities…[11]

Mission:data has already noted above that the Joint Utilities seek broad authority to apply to GBC users the data security requirements and termination rights that the Commission decided

---

[9] Joint Utilities Request for Clarification in Case No. 15-M-0180, dated November 21, 2018 at p. 2.

[10] *Ibid.* at p. 3.

[11] Joint Utilities Petition at p. 1-2.

previously should only be associated with EDI users. It is thus reasonable to ask what *additional* provisions will be concocted by the Joint Utilities over time to harm the adoption of DERs by skirting, modifying, extending or undermining Commission orders and rules. In the "business-to-business" process, the Joint Utilities have no incentive to accommodate any participant's suggested amendments to the DSA, nor do the Joint Utilities suffer any risk of penalty for denying any participant's suggested amendments to the DSA. As proposed, the "business-to-business" process is controlled entirely by the Joint Utilities; anyone who denies this reality could be accused of fanciful thinking. This is why numerous parties – including ESCOs,[12] DERs[13] and Mission:data – have repeatedly called for the Commission to intervene and prohibit what is in effect unilateral determinations about the DSA's terms by the Joint Utilities.

Several potential examples illustrate how pernicious the Joint Utilities' authority to modify the DSA at will could be. Suppose the Joint Utilities decide to remove billing information from its information technology platforms for DERs without justification. Billing information is used by DERs such as energy efficiency firms to monitor and estimate energy savings resulting from retrofits or behavioral changes over time. The Joint Utilities could create a false story to justify the withdrawal of billing information, such as that billing information purportedly requires additional cybersecurity protection and that the DSAs are being modified "out of necessity." DERs will have no choice but to accept the demands of the Joint Utilities because failure to sign a DSA will result in termination of all access to data. Furthermore, the DERs will have limited recourse at the Commission. If DERs were to file complaints to the Commission about the Joint Utilities' modifications to the DSA, the complaints would likely be denied due to the Commission's prior pre-approval of virtually all but the most egregious DSA amendments.

In another example, suppose the Joint Utilities decide to dramatically increase the audit requirements. The Joint Utilities could force DERs to accept costly on-site audits of DERs'

---

[12] See, e.g., *Final Comments of DSA Coalition Members on Proposed Data Security Agreement and Proposed Self-Attestation*. Case No. 18-M-0376, September 21, 2018 at p. 2 ("...the DSA Coalition strongly believes that core aspects of the DSA remain unresolved and should be revisited by the Commission in a full rulemaking proceeding").

[13] See, e.g., *Response of Advanced Energy Management Alliance on Petition for a Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers From Certain Cybersecurity Requirements.* Case No. 18-M-0376, December 21, 2018 at p. 5 ("DER Suppliers are hesitant to preemptively agree to provisions within the DSAs [in the business-to-business stakeholder process] that may or may not be found to be applicable...").

premises, and the Joint Utilities would send the bill for these unnecessary and inflated "audit services" to DERs to pay. Failure to pay what is in effect an extortionate fee would result in the DERs' termination of data access. This would be a convenient, perfectly permissible method for the Joint Utilities to act anti-competitively and disrupt DERs' businesses under the Joint Utility Petition. Technically, the Joint Utilities could argue that they are not in violation of the REV Track 2 Order's requirement that "basic data" be provided "at no cost" because cybersecurity practices are not implicated in the costs of providing "basic data." Such erroneous amendments to the DSA by the Joint Utilities would waste Commission time and resources over a period of months as complaint after complaint would be filed by DERs seeking relief. Instead of the Commission pro-actively preventing abuses by the state's Joint Utilities, as the Commission should be doing, the Joint Utilities Petition would, if approved, shortcut evidence-based Commission deliberations and shift the risk of abuses by the Joint Utilities onto DERs in advance of a hearing before the Commission.

Mission:data takes little comfort in the purported assurances advanced by some parties that the above activities "simply wouldn't happen." Put simply, the Joint Utilities seek to eliminate the due process rights of DERs. As co-equal market participants providing energy-related services to customers in New York, DERs have equal rights to participate in rulemaking dockets concerning Commission oversight over DERs that use GBC. That includes the right to participate in proceedings before the Commission without being subjected to what is, in essence, forced settlement negotiations with the Joint Utilities – the "business-to-business" process – where the Joint Utilities' whims will have already been pre-approved by the Commission. The Commission should deliberate and approve changes to the DSA *before* an agreement is foisted upon DERs by the Joint Utilities rather than *after* new terms and conditions are imposed.

e) The Commission has recognized that GBC users should have different terms and conditions than EDI users, but the Joint Utilities Petition seek identical terms and conditions.

Recognizing that GBC users' terms and conditions should be different from the DSA, the Commission took two recent actions. First, the Commission created the GB Working Group. In a February 7, 2019 notice, the Commission wrote:

> In order for the full benefits of GBC to be realized, responsibilities for third parties accessing data through GBC as well as the utilities' interaction with these third parties must be clearly articulated in a GBC terms and conditions agreement. The working group will focus only on the terms and conditions necessary for the useful and effective implementation of Green Button Connect in a consistent manner throughout the State.[14]

The above notice is dated February 7, 2019, some six (6) months *after* the DSA was "finalized." Second, the Commission's December 13, 2018 *Order Adopting Accelerated Energy Efficiency Targets* (the "EE Order") states:

> In order for the full benefits of GBC to be realized, responsibilities for third parties accessing data through GBC as well as the utilities' interaction with these third parties must be clearly articulated in a GBC Terms and Conditions agreement. This agreement must, among other things, include reasonable requirements for third parties to ensure the privacy and integrity of customers' data in relation to the risk associated with any breech [*sic.*] of customer data. Parties have had difficulty agreeing on terms and conditions, particularly with respect to data security. The utilities and Staff are directed to conduct a collaborative with DER providers and other interested parties to develop GBC terms and conditions that are consistent across utility service territories.[15]

Other Commission actions in favor of a distinction between EDI and GBC terms of use predate the DSA even further: the DER Oversight Order, dated October 19, 2017, states: "Additional methods of sharing data [beyond EDI] are already being implemented through technologies such as AMI and in other venues, including through Green Button Connect...Requirements and policies associated with receiving data through these systems will be developed in those venues."[16] The "venues" to which the Commission referred are not Case No. 18-M-0376, in which the DSAs were developed, but rather Case Nos. 13-E-0030 (Con Edison AMI approval order) and 14-M-0101 (REV, Distributed System Implementation Plans).

Approval of the Joint Utilities Petition would render the EE Order and the GBC Working Group moot. It is difficult to believe that the Commission would find the DSA acceptable to

---

14 *Notice of Green Button Connect Working Group*. New York Public Service Commission. Case No. 18-M-0084 et al. February 7, 2019 at p. 2.

15 *Order Adopting Accelerated Energy Efficiency Targets.* New York Public Service Commission. Case No. 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative. December 13, 2018 at p. 44.

16 DER Oversight Order at p. 28.

GBC users as written given the aforementioned inconsistencies with the EE Order. The Commission has not yet decided what GBC terms and conditions will be, and Mission:data believes the Commission should allow that effort to run its course, with a formal action ultimately taken by the Commission. The Joint Utilities' proposal to impose the DSA – and all future changes thereto – now for GBC users is inconsistent with Commission orders that clearly sought bespoke terms for GBC users.

f) Approving the Joint Utility Petition would disregard the EE Order's criteria for GBC terms and conditions.

The final conflict between the Joint Utilities Petition and Commission precedent has to do with the EE Order. The EE Order prescribed a specific principle about the terms and conditions for GBC users: "The terms and conditions should make it no more difficult for a DER provider, for whom a customer has provided consent, to access data than it is for the individual customer to access data."[17] To Mission:data's knowledge, no similar requirement exists for the terms of use associated with EDI users, such as ESCOs.

The GBC Working Group has not yet discussed exactly what GBC terms and conditions would satisfy this "no more difficult" standard, but it is safe to say that the DSA is unlikely to pass such a test. A brief comparison of the DSA with the method by which customers access their own information now is instructive. Individual customers can access their energy usage information on a utility's website without holding $5 million in cybersecurity breach insurance; without obtaining a SOC II audit of the customer's security practices and controls; without being contractually prohibited from making "derivations" of their energy usage information; and so on. On its face, the DSA is unquestionably more difficult for a DER to adhere to than it is for a customer to access his or her own information. In this respect, the Joint Utilities Petition conflicts with yet another Commission precedent.

[17] EE Order at p. 44.

4. Approving the Joint Utility Petition Would be an Abdication of the Commission's Duty

The Joint Utilities Petition asks the Commission to issue a ruling that the "business-to-business process...was appropriate for development of the DSA."[18] In essence, the Joint Utilities seek the Commission's bestowal of legitimacy upon the business-to-business process that led to the creation of the DSA.

At first, the appropriateness of the business-to-business process might sound reasonable because the Commission itself supported the business-to-business process in the *Order Initiating Proceeding* in Case No. 18-M-0376: "The Commission supports the business-to-business process..."[19] But upon closer examination, the business-to-business process has numerous flaws. The People of the State of New York, acting through the Legislature, vested the Commission with the authority to regulate utilities. The People did not grant *the utilities* such authority. Affirming the business-to-business process's appropriateness would be an abdication of the Commission's legal responsibilities. After all, it is the Commission that was designed to serve as an independent authority that affords due process to parties in a dispute. The Commission would cede its responsibility as a neutral overseer by delegating authority to the Joint Utilities.

Other parties have challenged the appropriateness and legality of the business-to-business process as well. The Retail Energy Supply Association ("RESA") recently argued the imposition of the DSA by the Joint Utilities on ESCOs would amount to a breach of the State Administrative Procedure Act ("SAPA").[20] Others have argued that if the Joint Utilities are permitted to unilaterally expand the scope of Case No. 18-M-0376 to DERs, serious procedural and due process concerns would be raised because DERs were not provided with sufficient notice of such discussions.[21] Mission:data believes that approving the appropriateness of the

---

[18] *Ibid.*

[19] Case No. 18-M-0376, Order Instituting Proceeding, dated June 14, 2018 at p. 3.

[20] *Response of RESA to the Joint Utilities' Petition for Declaratory Ruling Regarding Their Authority to Discontinue Utility Access to Energy Services Companies in Violation of the Uniform Business Practices*. Case Nos. 98-M-1343 and 18-M-0376, filed December 21, 2018.

[21] See, *e.g., Corrected Comments of Advanced Energy Management Alliance on Data Security Agreements and Self-Attestation Forms for Distributed Energy Resource Suppliers*, Case No. 18-M-0376, dated December 18, 2018 at p. 5; *Final Comments of DSA Coalition Members on Proposed Data Security Agreement and Proposed Self-Attestation*, Case No. 18-M-0376, New York Retail Choice Coalition, filed September 21, 2018 at p. 7.

business-to-business process would be a dereliction by the Commission, irreparably harming the Commission's credibility on this and future cases.

Despite the Joint Utilities' claim that "concessions" on the DSA stemming from the utility-controlled negotiations are themselves evidence of due process, the reality for DERs is quite different. Many DERs feel the business-to-business process was coercive. The Joint Utilities cite large numbers of meetings, stakeholders and written feedback as evidence of the DSA's thoroughness and legitimacy. However, for DERs, the temerity of these claims is extraordinary. How can the Joint Utilities be allowed to use a stakeholder's mere attendance at a meeting as justification for the Joint Utilities' position? If allowed to stand, stakeholders could be disincentivized from attending any stakeholder meeting in the future, lest their presence at meetings, or their opinions made known therein, be misrepresented by the Joint Utilities.

While it is true that the Commission initiated the business-to-business process, it is not necessarily true that the Commission must accept its result. The Commission's original approval described in the *Order Initiating Proceeding* of Case No. 18-M-0376 was limited to *initiating* a business-to-business discussion as a *possible* mechanism to resolve disputes over data security topics. In Mission:data's view, the Commission can, without contradiction, support a *process* and not support its *outcome*.

5. The Joint Utilities Petition Should Be Denied Because the DSA Contains Vague Language That Immediately Put DER Providers In Violation Of Its Terms

By approving the Joint Utilities Petition, the Commission would turn a blind eye to disturbingly vague language in the DSAs. At least two fatally-flawed sections of the DSA would immediately result in GBC users, such as DERs, being in violation.

The first such clause is Section 14(a) of the DSA, which reads:

> ESE shall not create or maintain data which are derivative of Confidential Utility Information except for the purpose of performing its obligations under this Agreement or as authorized by the UBP or UBP DERS. For purposes of this Agreement, the following shall not be considered Confidential Utility Information or a derivative thereof: (i) any customer contracts, customer invoices, or any other documents created by ESE that reference estimated or actual measured

> customer usage information, which ESE needs to maintain for any tax, financial reporting or other legitimate business purposes consistent with the UBP or UBP DERS; and (ii) Data collected by ESE from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESE or its partners.[22]

The first sentence cited above is the most striking. The prohibition on creating or maintaining "derivatives" of energy data would do two things. First, "derivations" are so broadly defined as to encompass practically every processing function of customer-authorized software programs: counting time-series energy usage records in a database; creating daily averages of energy use for comparison purposes; correlating energy use with outdoor temperature in order to assess weather-normalized energy usage patterns; and so on. The phrase "for the purpose of performing its obligations under this Agreement" does not release DERs from the DSA's handcuffs; performing the DSA's obligations refers to the DERs' obligations *to the utility*, not to the customer. And neither does the phrase "as authorized by the UBP or UBP DERS" help matters because the UBP-DERS similarly does not tie the DERs' acceptable use of customer data to the scope of the customer's authorization. Essentially, all DER software applications with which Mission:data is familiar would immediately be in breach of the DSA.

Second, the prohibition of "derivatives" would clearly conflict with customer-authorized purposes. What if customers *want* to DERs to create derivative energy information in order to receive recommendations based upon that analysis? Creating derivatives should be encouraged by the Commission, not prohibited. After all, engaging customers with new data analysis techniques that help save energy was one of the primary goals of REV. And yet, the DSA is inherently blind to the scope of the customer's authorization to access information.

Even if the Joint Utilities were to choose not to enforce the DSA for violations of Section 14(a), the damage will have been done: DERs would suffer unacceptable and unnecessary business uncertainty. In Greek mythology, the Sword of Damocles refers to the precarious anxiety experienced by Damocles who takes the King's seat of power: Damocles notices a sword's blade is held above his head, supported only by a single horse hair that could break at any moment. Similarly, DERs will experience the continuous threat of business interruption because enforcement of the DSA would be entirely up to the whims of the Joint Utilities.

---

[22] DSA, Section 14(a) at p. 9.

The second fatal flaw of vague language in the DSA involves customer consent. Section 4 reads:

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

One portion of the UBP-DERS, Section 2(C)(B)(3), reads: "A DER supplier shall retain, for a minimum of two years or for the length of the sales agreement, whichever is longer, verifiable proof, including but not limited to a recording or signed writing, of authorization for each customer."

Under the Joint Utilities Request for Clarification, Section 2(C) in its entirety would become applicable to GBC users, including the citation above. Thus, DER suppliers would be obligated to hold the customer's authorization for inspection by the Commission for a minimum of two years. That might sound reasonable, but according to the GBC technical standard, it is the *utility*, not the DER, that receives the customer authorization. The DER has no way of knowing that an authorization has occurred until it receives confirmation *from the utility*. DERs could certainly retain the utility's electronic representation of that consent, but the utility's electronic representation is not the original, and so it may not meet the definition of "verifiable." In other words, the DER could immediately be in breach of the DSA.

6. The Joint Utilities' Response to Mission:data's Petition for Declaratory Ruling

On December 21, 2018, the Joint Utilities filed a *Response to Mission:data's Petition for Declaratory Ruling* (the "Joint Utilities Response") in Case Nos. 15-M-0180 and 18-M-0376. Mission:data will briefly reply to the Joint Utilities Response since it appeared as Attachment 5 in the Joint Utilities Petition.

(a) The Joint Utilities argue that Mission:data's Petition for Declaratory Ruling is moot. If so, then so is the Joint Utilities Petition.

As mentioned above, the EE Order directed Department of Public Service Staff ("Staff") to convene a collaborative with interested stakeholders specifically to develop GBC terms and conditions.[23] The Joint Utilities Response cited the EE Order and concluded: "Mission:data's Petition is moot because the Joint Utilities will be working with Staff and interested stakeholders, including presumably Mission:data, to develop appropriate GBC cyber security and customer data protections."[24]

The Joint Utilities' reasoning is deeply troubling. The Joint Utilities are arguing that a Commission order, i.e. the DER Oversight Order, should not be enforced by the Commission merely because a *related* proceeding is ongoing. Affirming the Joint Utilities' argument would set a dangerous precedent, crippling the Commission's powers to enforce innumerable rules and orders from the past. How many proceedings are currently pending before the Commission that are related – even closely related? It is almost impossible to count. The net effect of the Joint Utilities' reasoning is that wide swaths of the Commission's existing rules and orders would be rendered impotent.

Also, rejecting Mission:data's petition because it is allegedly "moot" cuts both ways: the Commission must also simultaneously reject the Joint Utilities Petition as being moot. The Joint Utilities seek authority under the UBP-DERS to enforce the DSA over any entity that uses GBC. If the Commission's consideration of GBC terms and conditions in an ongoing proceeding is reason to deny Mission:data's petition concerning the DER Oversight Order's cybersecurity requirements, then the Commission must also deny the Joint Utilities' request to enforce the DSA against GBC users because of ongoing proceedings discussing cybersecurity requirements. Both Mission:data and the Joint Utilities seek guidance from the Commission on the applicability of the DER Oversight Order; it would be illogical for the Commission to apply different standards to the respective petitions of Mission:data and the Joint Utilities.

(b) The Joint Utilities are incorrect that other jurisdictions require adherence to terms and conditions similar to the DSA.

---

[23] EE Order at p. 44.

[24] Joint Utilities Response at p. 2.

In a presentation at a November 18, 2018 workshop, Mission:data presented information about other state public utility commissions and the range of requirements that utilities in other jurisdictions impose of DERs that receive customer energy information. The Joint Utilities attempt to dismiss this information as being inaccurate, but in fact, the policies cited show how out of step the DSA is with the norms of other jurisdictions. Many terms in the DSA simply do not exist in other jurisdictions, as explained below. Furthermore, to the extent Commonwealth Edison and Pacific Gas & Electric have required certain terms beyond their respective commission-approved tariffs, then those additional requirements are unenforceable because commission orders and tariffs supersede. Any requirements on GBC users that go beyond commission orders and tariffs in the states mentioned by the Joint Utilities represent exactly the type of extrajudicial seizure of authority about which Mission:data is very concerned could occur in New York.

The Joint Utilities cite Commonwealth Edison's "Data Services Handbook for Third Parties" that references a non-disclosure agreement ("NDA"). The NDA cannot be found either on Commonwealth Edison's website or the registration materials that third parties receive,[25] so it impossible to know its precise contents. Nevertheless, the NDA is unenforceable to the extent it conflicts with Illinois's Commission-approved tariff that governs GBC or the Commission decision authorizing GBC. Contrary to the Joint Utilities' claims, the tariff's requirements of third party registration with Commonwealth Edison are much simpler than those in the DSA. Third parties (i.e., GBC users) must (i) meet certain confidentiality requirements, as explained below; (ii) complete interoperability testing with the utility and (iii) submit a registration with contact information. Regarding confidentiality, third parties must:

> treat such data specific to such retail customer that it accesses and/or retrieves as confidential information and ensure the confidentiality of such data specific to such retail customer in accordance with all applicable statutes and regulatory orders or rules…
>
> agree that such data specific to such retail customer must not be sold or licensed to any other entity for any purpose…

[25] In spite of the "Data Service Handbook" referencing the NDA, a third party registrant at Commonwealth Edison reported to Mission:data that no NDA was required.

> agree that such data specific to such retail customer must not be used for commercial purposes not reasonably related to the conduct of the Company's business.[26]

Third parties are also permitted to disclose customer energy data to their "contracted third party vendors or its affiliates" so long as such disclosure is consistent with the customer-specified purpose.[27]

That is the extent of Illinois's non-disclosure and cybersecurity requirements of GBC users. Mission:data notes that none of the following elements of the DSA are present in Commonwealth Edison's tariffs or required agreements (and this is not exhaustive):

- adherence to specific, named cybersecurity standards including NIST SP 800-53 and ISO 27001 / 27002;
- a SOC II audit, or any other on-site audit rights for the utility to inspect the third party's facilities;
- notification to the utility of a data security incident;
- prohibitions on creating or maintaining "derivations" of energy data;
- prohibitions on sharing energy data with "third-party representatives" unless consistent with the customer-authorized purpose;
- return or destruction of customer energy data following termination; and
- cybersecurity breach insurance

The Joint Utilities state that Commonwealth Edison requires "clear provisions relating to data loss or breach," but the above terms are clearly *not* "akin to the types of provisions in the DSA."[28]

The Joint Utilities also cite California's commission and Pacific Gas & Electric ("PG&E") as having rules consistent with the DSA. However, this claim falls apart upon scrutiny. The Joint Utilities appear to argue that the DSA is consistent with California policy

---

[26] Commonwealth Edison Company. Rate DART Data Access and Retrieval Tenets, effective May 23, 2016. 4th Revised Sheet No. 229-230.

[27] Illinois Commerce Commission. Final Order in Docket No. 15-0073, dated March 23, 2016 at p. 15.

28 Joint Utilities Response at p. 18.

merely because the California commission's privacy rules are "strict" and "lengthy." California's privacy rules are indeed lengthy, but it doesn't necessarily follow that California's policies are consistent with the DSA. Mission:data's presentation at the November 18, 2018 workshop included a table showing "cybersecurity requirements." Under California, it said "reasonable safeguards." Mission:data stands by the words in our presentation. When referring to requirements specific to cybersecurity measures – and not to *all* conceivable terms and conditions – the lengthy California privacy rules say nothing about encryption, SOC II compliance, NIST standards, ISO 27001, or cybersecurity breach insurance. Instead, Section 8, Data Security, of California's privacy rules read simply: "Covered entities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure."[29] This is symmetrical with California Senate Bill 1476's (Padilla, 2010) requirement that utilities provide "reasonable security procedures and practices."[30]

The Joint Utilities also opine that California's policies "apply not only to the third party registering to use GBC, but also their agents, contractors and subcontractors."[31] That is true, but third parties may disclose customer data to agents, contractors and subcontractors so long as the customer consents. And when customer consent is provided for such sharing, California rules deviate substantially from the DSA's provisions. Specifically, California rules differ from the DSA in terms of (i) advance written subcontractor agreement to the DSA (including cloud hosting providers); (ii) flow-down provisions surrounding audit rights and assistance to the utility; and (iii) information security programs as specified on the self-attestation. While Mission:data does not deny that California's privacy rule is lengthy, it is substantially different from the DSA.

Finally, the Joint Utilities cite PG&E's terms and conditions for GBC users as including an insurance requirement. The Joint Utilities are correct: Mission:data was unaware that PG&E's terms require third parties to "insurance coverage...sufficient to cover any liabilities or claims for

---

[29] California Public Utilities Commission. Decision D.11-07-056 at Attachment D, p. 11. Available at http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/140370.PDF.

[30] California Senate Bill 1476 (Padilla, 2010). As cited in *Ibid.*, Attachment A at p. 2.

[31] Joint Utilities Response at p. 18.

damages that may result…."[32] However, the Joint Utilities' argument is moot because this requirement is unenforceable, as it is inconsistent with both the California commission's privacy rules and PG&E's tariff known as Rule 25. (Mission:data will be asking the California commission to order PG&E to rescind any terms and conditions that are in conflict with, or go beyond, commission orders.) As stated above, Mission:data's overriding concern is that, absent clear Commission direction, utilities will take every opportunity to seize additional powers over third parties and require onerous terms that inhibit DER growth. Rather than support the Joint Utilities argument, the examples cited further validate Mission:data's concern that the business-to-business process is deeply flawed and that utilities in any state should not be permitted to have control over the terms and conditions governing their data-exchange relationships with DERs.

7. If the Joint Utilities Petition is Approved, the Commission Must Rescind Substantial Portions of REV

If the Commission votes to approve the Joint Utilities Petition, the Commission should be aware of the repercussions. By granting substantial new authorities to utilities, the Commission will be affirming precisely the opposite principle of what REV envisioned: a dynamic, third-party DER driven market. Instead of utilities serving as "distribution system platforms," which connotes the *enabling* of future innovations, utilities will inhibit data-driven DER adoption while citing "cybersecurity" as a justification. To use an analogy, instead of an open internet, the Commission will be opting for the "walled garden" approach of American Online in the 1990s in which consumers only have access to the services that are vetted, approved and maintained by the utility.

Customer choice of DERs was essential to the Commission's REV decisions over the years. The Commission stated that "the objective of REV is to create a marketplace for DER based upon consumer information and choice."[33] For similar reasons, the Commission also

---

[32] Available at: https://www.pge.com/includes/docs/pdfs/myhome/addservices/moreservices/sharemydata/ShareMyData_Platform_TermsofUse.pdf

[33] Order Adopting Regulatory Policy Framework and Implementation Plan. Case No. 14-M-0101, February 26, 2015 at p. 66.

opposed utility ownership of DERs: "We do not generally favor utility ownership of DER assets. We are persuaded that unrestricted utility participation in DER markets presents a risk of undermining markets more than a potential for accelerating market growth."[34] The Commission noted that many DERs "suggest that anything short of a robust flow of information would allow utilities to exercise market power sufficient to stifle third-party entry."[35] Given the DSAs' one-sidedness and departure from other states' norms regarding third party terms and conditions, it would appear that DSAs are precisely the stifling instruments that the Commission had feared would inhibit data-driven DER adoption.

If the Commission approves the Joint Utilities Petition, then the Commission must also acknowledge that several core tenets of the REV initiative are essentially dead. It is difficult to see how data-driven, third party DERs will "animate the market" when the Joint Utilities are permitted to stifle innovation with the DSAs as written.

8. Recommendations For Bespoke GBC Terms and Conditions

Although Mission:data strongly urges the Commission to reject the Joint Utilities Petition, Mission:data understands that merely rejecting the petition does not solve all the challenges faced by the Commission. Numerous underlying problems will persist despite a rejection of the Joint Utilities Petition. Mission:data believes that, in order to constructively resolve the issues before the Commission, root causes must be addressed. Toward that end, Mission:data provides the following recommendations.

First, the relationship between customers, DERs and utilities needs to be clearly understood. The Joint Utilities fundamentally misread the relationship between themselves and DERs. Many DERs that seek to use GBC are not utility vendors like Opower, commodity suppliers like ESCOs, or government agencies such as community choice aggregators ("CCAs"). The reason why the Joint Utilities' boilerplate contracts and cybersecurity requirements should not apply in the same way to DERs is that customers are totally free to choose or decline DER products and services. No one is requiring customers to buy DER products or services like smart

---

[34] Ibid at p. 67.

[35] Order Adopting Regulatory Policy Framework and Implementation Plan. Case No. 14-M-0101, February 26, 2015 at p. 57.

thermostats, energy efficiency smartphone "apps" or smart power strips. If a customer buys such a product, it should not be the utility's responsibility to prevent downstream harms that might result.

In one sense, the Joint Utilities are correct when they argue that the DSA is "routine" and typical of the utility industry: utility vendors, ESCOs and CCAs are required to sign agreements similar to the DSA. But the Joint Utilities fail to understand why DERs that seek to use GBC are different. GBC users are not the utility's vendors. Once customer data is released to a third party entity, it is that entity who is solely responsible for any harms the customer might experience. For REV to succeed, the dynamism of a competitive market must be allowed to flourish. But Mission:data is very concerned that REV will not succeed so long as utilities perceive themselves as responsible for the entirety of the customer's commercial relationships with DERs that utilize customer data.

In telecommunications, there is the concept of the "demarcation point" which separates the monopoly utility from the competitive market. The telephone box on the side of a customer's home is the termination point of the local exchange's copper wire. The telco is responsible for the wire up to that point. Beyond that point, the telco is not responsible. Often referred to as "inside wiring," the customer is responsible for its upkeep and maintenance. Customers are also free to choose whatever landline or portable phone they want. A similar demarcation point needs to be defined for utilities in New York in order for REV to succeed. Mission:data would argue that customer's consent to share data with a third party should mark that demarcation point.

(a) Staff's distinction between "system risk" and "data misuse risk" is important. The Commission should require utilities to own their system risk but disown any downstream data misuse risk.

In a recent workshop, Staff articulated the difference between "system risk" and "data misuse risk." System risk is the cybersecurity threat utilities face by having any entity access their I.T. systems. Data misuse risk is the risk that a customer-authorized third party will abuse the customer's privacy rights using information collected from the utility. This distinction is a positive step forward, but the Commission should go further and require utilities to be responsible for their own system risks while explicitly waiving their responsibilities to mitigate data misuse risks by placing data misuse risks solely on DER suppliers.

Regarding system risks, Mission:data believes the utilities should be solely responsible for their I.T. systems. If a utility's GBC platform is breached, it is the utility's responsibility. Similarly, a breach of the utility's customer web portal would be the utility's responsibility – not the users of the platform. The GBC standard ensures that customer data is only released with customer consent, and that such release occurs via Transport Layer Security, i.e. an encrypted channel. If the GBC platform is successfully attacked, that can only be because the utility has not adequately prepared and managed its systems. Shifting system cybersecurity responsibilities onto GBC users would therefore be inappropriate.

Second, the Commission should not conflate the system security risks of GBC with EDI. The Joint Utilities have falsely claimed that all interactions with utility I.T. systems pose identical risks: "These risks include the ability of DERs to harm a utility system during the regular exchange of information as well as the potential loss of customer data. This risk exists not only using the EDI platform, but also other electronic data platforms, including GBC."[36] As was explained in detail during a recent stakeholder workshop, GBC, unlike EDI, requires utility-processed customer consent prior to releasing data.

As for data misuse risk, Mission:data argues that the Commission should explicitly waive the Joint Utilities' liability, so long as the data is transferred pursuant to customer consent and is encrypted in transit. This waiver is the only way to remove the utilities from taking a "policeman"-type role over GBC users. While it is reasonable and necessary for utilities to "police" the data management practices of their vendors, the same is not true of GBC users. Without an explicit waiver by the Commission, it is unlikely that we will make headway in constructively resolving these issues.

(b) Look to California for enforcement procedures.

One of Mission:data's gravest concerns about the DSA is the lack of due process afforded to DERs that use GBC. When a dispute arises, the Joint Utilities will have full control over the DERs' fate. California wrestled with this problem in 2013 and found a good solution, portions of which have been adopted in states such as Colorado, Illinois and Texas.

---

[36] Joint Utilities Response at p. 15.

First, California established eligibility criteria for third parties. To be eligible, third parties must:

1. Provide utilities their contact information, including federal tax identification number, so as to uniquely identify third parties across the three investor-owned electric utilities;
2. Demonstrate technical capability to interact with the GBC platform;
3. Acknowledge receipt of the commission's privacy rules; and
4. Not be present on the commission's list of "banned" third parties.

Next, the California commission established a process by which utilities can report to the commission a "reasonable suspicion" of a third party's violation of privacy rules, and the commission will investigate. If the third party is found to have violated the rules, the commission can place the offending third party on the "banned" list. It is important to note that the utility does not have the ability to unilaterally revoke a third party's access; it is only by reporting a suspected violation that the utility "passes off" responsibility for investigation and enforcement to the commission.

California's enforcement mechanism has served the state well. Since the release of the investor-owned utilities' GBC platforms in 2016, Mission:data understands that several suspected violations have been reported to the commission, although to our knowledge, no third party has yet been banned. Customers may seek redress before the commission but it is not the utility's responsibility to vet third parties or enforce privacy policies against third parties. According to the commission's privacy rules, "After a secure transfer, the electrical corporation shall not be responsible for the security of the covered data or its use or misuse by such third party."[37]

9. Conclusion

Mission:data hopes that the information provided herein is helpful as the Commission deliberates these issues. Thank you for the opportunity to provide comments.

[37] California Public Utilities Commission, D.11-07-056 at Attachment D, p. 9.

Respectfully submitted,

Michael Murray, President

Mission:data Coalition
1752 NW Market St #1513
Seattle, WA 98107
(510) 910-2281 (phone)
michael@missiondata.io