November 30th, 2018

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, In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products

Attached is Mission:data Coalition's Petition for a Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements. If you have any difficulty viewing the attached 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

Petition of Mission:data Coalition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements

1. Introduction

Pursuant to 16 N.Y.C.C.R. Section 8, Mission:data Coalition ("Mission:data") hereby petitions the Public Service Commission ("PSC" or "Commission") to issue a declaratory ruling affirming its October 19, 2017 Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers in Case 15-M-0180 ("DER Oversight Order").[1] Specifically, the declaratory ruling should affirm that the Commission expressly prohibits any utility offering Green Button Connect ("GBC") from requiring Distributed Energy Resource Suppliers ("DER Suppliers") to sign Data Security Agreements, and related documents such as a Self-Attestation of Information Security Controls (together, the "DSAs"), as a condition of using GBC. A declaratory order is appropriate and necessary because there is a direct conflict between the Commission's language in the DER Oversight Order and the utilities' recently-imposed, extrajudicial requirement that DER Suppliers comply with the DSAs

[1] Case 15-M-0180. In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products, Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Providers and Products, dated October 19th, 2017 at Appendix A, p. 7.

developed in this proceeding as a condition of accessing customer data via the Green Button Connect platform. This directly contravenes the plain language of the DER Oversight Order that exempts DER Suppliers that use GBC from those cybersecurity requirements. The DER Oversight Order section that discusses data security requirements states clearly that "This section does not impose any obligations on DER suppliers that do not request or receive data using EDI [Electronic Data Interchange]".[2] In other words, the DER Oversight Order specifically prohibits utilities from requiring DER Suppliers that do not use Electronic Data Interchange ("EDI") to abide by certain cybersecurity requirements. In violation of the DER Oversight Order, the Joint Utilities are currently requiring DSAs to be signed by DER Suppliers, regardless of the platform used or the type of data exchanged with DER Suppliers. Accordingly, Mission:data respectfully requests the Commission address and resolve this conflict by affirming the DER Oversight Order.

2. Chronology and Context

A. Chronology

On May 12th, 2015 in Case 15-M-0180, the proceeding relevant to the instant proceeding involving establishing an oversight framework and uniform business practices for Distributed Energy Resource Suppliers, the Commission held its first technical conference to discuss rules regarding Commission regulation and oversight of DER providers and products.

On July 28th, 2015 in Case 15-M-0180, Commission Staff issued a proposal for DER oversight and sought input from parties. Over the next year, comments were submitted by multiple parties and additional technical conferences were held.

On April 11th, 2017 in Case 15-M-0180, Staff issued a whitepaper concerning DER oversight and sought comments and reply comments from parties. Again, input and expertise was provided by interested stakeholders.

---

[2] *Id.*

On October 19th, 2017, after considerable investment of time and resources from stakeholders and careful consideration by the Commission, the Commission issued the DER Oversight Order. In the section addressing protection of customer information the order states, "This section does not impose any obligations on DER suppliers that do not request or receive data using EDI…"[3]

On November 21st, 2017 in the DER Supplier oversight case, Case 15-M-0180, the Joint Utilities filed a Request for Clarification in which the Joint Utilities "respectfully request that the Commission clarify that Section 2C, Subparts A, B, D, E, F and G apply to DERS requesting customer data not only through EDI, but also include other utility platforms for data access."[4] This is relevant for Mission:data's petition for a declaratory ruling in this case because in the Request for Clarification the Joint Utilities acknowledge the DER Oversight Order prohibits imposition of the DSAs requirements on DER Suppliers accessing customer data through the GBC platform.

On July 2nd, 2018, Mission:data filed comments in this proceeding, Case No. 18-M-0376, asking for the Commission to clarify what is required of DER Suppliers that seek to access customer data held by the utility. Citing the fact that Consolidated Edison Company of New York ("ConEd") is requiring DER Suppliers that access customer data to sign a Data Security Agreement that is identical to that used for Energy Services Companies ("ESCOs"), despite the DER Oversight Order not requiring that DSAs be signed by DER Suppliers, Mission:data asked, "while the Order [Instituting Rulemaking in 18-M-0376] ostensibly pertains only to 'energy services entities,' it is reasonable for DER Suppliers to wonder what regulations apply to them, what attestations of DER Suppliers may be required..."[5]

On September 24, 2018, the Department of Public Service Report on the Status of the Business-to-Business Collaborative to Address Cybersecurity in the Retail Access Industry ("Staff Report") in this proceeding made recommendations aligned with the Commission's conclusions in its DER Oversight Order. The Staff Report acknowledges the differences

---

[3] *Id.*

[4] Joint Utilities Request for Clarification dated November 21st, 2017 at p. 3.

[5] Comments of Mission:data Coalition dated July 2nd, 2018. Case No. 18-M-0376, Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, at p. 2.

between DER Suppliers and Energy Service Providers ("ESEs") and between the EDI and GBC platforms: "Second, where discussions with DERS have occurred, it is apparent that, in at least some instances, DERS warrant different treatment than the ESEs and perhaps even other DERS. For example, some DERS utilize different forms of electronic communication with the utilities and/or may receive different customer data points as compared to an ESCO. For these reasons, Staff recommends that a similar business-to-business process be utilized to refine the existing DSA to make its terms more aptly applicable to DERS." The Staff Report also states, "In the meantime, however, Staff recommends application of the revised DSA to DERS with EDI type interfacing as the most appropriate articulation of cyber controls to be applied to this industry."[6] The Staff Report does not require the revised DSAs be required for the GBC interface and therefore remains consistent with the critical distinctions contained within the DER Oversight Order.

On October 16th, 2018, based on observing that ConEd and other utilities were requiring that DER Suppliers agree to DSAs, as a condition of accessing customer data via GBC, which directly contravenes the plain language of the DER Oversight Order, Mission:data filed a timely response to the November 21st, 2017 Joint Utilities Request for Clarification in Case 15-M-0180.

On November 9th, 2018, a Petition of the Joint Utilities for Declaratory Ruling Regarding their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices ("Joint Utilities' Petition") was filed in the instant case. The Joint Utilities' Petition appears to conflate all types of energy services providers, thus including DER Suppliers within the scope of the requested relief, contrary to Commission order and precedent. If granted, the Joint Utilities' Petition would impose unnecessary and significant regulatory burdens on DER Suppliers.

B. Context

Green Button Connect ("GBC") is a nationally-recognized technical standard designed to enable customers to share their energy data held by a utility with a third party DER Supplier. The Commission has adopted GBC requirements for all utilities with advanced metering infrastructure ("AMI") as a way to "animate" DER markets and pursue Reforming the Energy

---

[6] Staff Report at p. 7-8.

Vision ("REV") objectives. Various Commission rulings require GBC, including, but not limited to, the March 17th, 2016 Order approving ConEd's AMI business plan,[7] the April 20th, 2016 Order adopting Distributed System Implementation Plan Guidance[8] and the May 19th, 2016 REV Track 2 Order.[9] GBC is contrasted with Electronic Data Interchange ("EDI"), which, according to the DER Oversight Order, is a mechanism in New York "used in retail access programs to switch customers from one supplier to another or to exchange customers' history, usage or billing data between a distribution utility or Meter Data Service Provider and an ESCO."[10]

ConEd is the first New York utility to implement GBC, although GBC is not yet "live." In ConEd's July 29th, 2016 AMI Customer Engagement Plan, ConEd stated that GBC would "go live" in January, 2018.[11] However, that did not occur. In a subsequent filing dated October 2nd, 2017, ConEd issued a revised schedule indicating that GBC would "go live" in January, 2019.[12] In a filing on April 30th, 2018, ConEd stated "There are currently eight third parties going through the 'Share My Data' onboarding process, which includes successfully completing the Vendor Risk Assessment, signing the Data Security Agreement, and successfully completing technical onboarding."[13]

As the Staff Report notes, DERS "warrant different treatment" than other energy service providers.[14] For example, the DER Supplier market is a nascent one, and DER services are optional for the customer. The DER market is expected to generate many public policy and consumer benefits once GBC is operational. In contrast, ESCOs, once selected by a customer, supply basic energy commodity services, compete in a more regulated market, and have a long

---

[7] Case Nos. 13-E-0050, 13-E-0030 and 13-G-0031. New York Public Service Commission, Order Approving Advanced Metering Infrastructure Business Plan Subject to Conditions, dated March 17th, 2016 at p. 41-42.

[8] Case No. 14-M-0101, Reforming the Energy Vision, Order Adopting Distributed System Implementation Plan Guidance, dated April 20th, 2016.

[9] Case No. 14-M-0101. New York Public Service Commission, Order Adopting a Ratemaking and Utility Revenue Model Policy Framework, dated May 19, 2016 at p. 140-143.

[10] DER Oversight Order, Appendix A at p. 2.

[11] ConEd, AMI Customer Engagement Plan. Case Nos. 15-E-0050, 16-E-0060 and 14-M-0101. July 29, 2016 at p. 38.

[12] ConEd and Orange and Rockland Utilities Green Button Connect Phase 2 Report. Case Nos. 15-E-0050, 16-E-0060 and 14-M-0101. October 2nd, 2017 at p. 8.

[13] ConEd, AMI Metrics Report. Case No. 16-E-0060 et al. at p. 8.

[14] Staff Report at p. 7-8.

history in New York. Burdening DER Suppliers with the same onerous cybersecurity requirements as those required of ESCOs is not justified.[15] Additionally, the Commission lacks evidence that DER Suppliers pose similar cybersecurity risks. Mission:data is not opposed to appropriate consumer protections for customer data; however, they should be appropriately tailored to the services provided and the actual risks involved. Mission:data supports Staff's recommendation that the DSAs be modified to "make its terms more aptly applicable to DERS."[16] The DSAs for ESCOs are onerous and inappropriate for DER Suppliers and will delay the development of the DER Supplier market to the detriment of consumers. Access to customer energy usage data via GBC is crucial for DER Suppliers to offer services.

3. ConEd is requiring DER Suppliers using Green Button Connect to sign Data Security Agreements.

Following the creation of Case No. 18-M-0376, "Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place," the utilities, ESCOs and Commission Staff began a "business to business" negotiation to create a DSA, self-attestation regarding cybersecurity controls and a "vendor risk assessment" form (collectively, the "DSAs") to be required of ESCOs. The DSAs were finalized by the parties in August, 2018. The documents are posted on the Commission's website.[17]

The Joint Utilities are putting the DSAs into practice, requiring ESCOs to execute the forms. According to the Staff Report on the status of the "business-to-business collaborative" that led to the revised DSAs, the Joint Utilities "assert authority under the Uniform Business Practices (UBP) to require these basic level cyber security requirements of ESEs [energy services entities] that interface with the utilities' systems."[18]

---

[15] These differences are thoroughly explored in Case No. 15-M-0180, the DER Oversight proceeding, and support the Commission's decision not to impose identical cybersecurity requirements.

[16] *Id.*

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

[18] Case No. 18-M-0376. Department of Public Service Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry, dated Sept 24th, 2018 at p. 3.

Of importance to Mission:data is that ConEd, who is the first New York utility to offer GBC, also requires DER Suppliers wishing to use GBC, and not merely ESCOs that use EDI, to execute the DSAs. According to the Joint Utilities, the newly-finalized DSAs are meant to apply to all energy services entities ("ESEs"), not just ESCOs and their I.T. contractors. According to the final DSA dated August 16th, 2018, an ESE is an entity which "includes but is not limited to ESCOs, Direct Customers, DERS and contractors of such entities..."

Two documents make it clear that the Joint Utilities are presently acting as though the DSA applies to DER Suppliers who seek to access customer data via GBC. A set of "Frequently Asked Questions" drafted by the Joint Utilities explains: "All ESEs, including ESCOs, Direct Customers, DERS and EDI Providers that electronically exchange data with the Utility must enter and abide by the DSA."[19] In addition, an email posted on the Commission's website from Joint Utilities representative Mary Krayeske dated August 16, 2018, states: "The Joint Utilities consider the DSA, and the previously sent Self-Attestation, to be final. ESEs must submit the completed and signed Self Attestation by August 24, 2018."[20] Mission:data member companies also report that ConEd is requiring GBC registrants to execute the DSA. Furthermore, representatives from ConEd at the November 14th, 2018 stakeholder forum in Albany, NY similarly confirmed that ConEd requires the DSAs for DER Suppliers who wish to access customer data via GBC. The November 9th, 2018 Joint Utilities' Petition escalates DER Supplier business risk even further.

4. Contrary to the Joint Utilities' claims, the DER Oversight Order does NOT require DER Suppliers to sign Data Security Agreements as a condition of accessing customer data via Green Button Connect.

Whereas ConEd requires GBC registrants to execute the DSAs, the DER Oversight Order does not state any such requirement. In fact, the DER Oversight Order specifically *exempts* DER

---

[19] See http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/4a24d0d51395b1f8852582a2004398a3/$FILE/54482093.pdf/DSA-SA%20JU%20FAQ%2020181004.pdf.

[20] See http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/4a24d0d51395b1f8852582a2004398a3/$FILE/99498797.pdf/DSA-SA%20JU%20Message%2008-16-2018.pdf.

Suppliers from cybersecurity requirements such as those in the DSAs, provided that the DER Supplier uses GBC rather than EDI.

The Uniform Business Practices for DER Suppliers ("UBP-DERS"), adopted as part of the DER Oversight Order, states in Section 2C, Customer Data:

> A. Applicability. **This Section establishes practices for release and protection of customer information by distribution utilities or DSPs to DER suppliers using EDI** [*emphasis added*]. It also identifies the content of information sets transmitted using EDI standards. The distribution utility or DSP and a DER supplier shall use standards, systems, and protocols developed for these purposes for transmittal of customer information. **This section does not impose any obligations on DER suppliers that do not request or receive data using EDI** [*emphasis added*]...
>
> F. 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.
>
> G. 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.

Sub-sections (F) and (G), on the NIST Cybersecurity Framework and Data Security, respectively, are contained within Section 2(C) and are therefore not required of DER Suppliers that "do not request or receive data using EDI."

By requiring the DSAs of DER Suppliers using GBC, ConEd's actions contravene the plain language of the DER Oversight Order. Whereas ConEd is presently acting as if the DER Oversight Order requires ConEd to, in turn, require executed DSAs of DER Suppliers, in fact the opposite is true. The Commission expressly declined to make "data security requirements" of ESCOs applicable to DER Suppliers, so long as DER Suppliers do not use EDI.

5. ConEd is in violation of the DER Oversight Order, and the Commission should prohibit utilities from requiring DSAs of DER Suppliers using GBC unless and until the Commission formally modifies the UBP-DERS.

Commission orders are, of course, legally binding upon regulated entities. The DER Oversight Order was approved by the Commission on October 19th, 2017. On page 1 of the Uniform Business Practices for DER Suppliers ("UBP-DERS"), the following appears in large

type: "EFFECTIVE DATE: DECEMBER 1, 2017." Therefore, the DER Oversight Order has taken full effect.

What makes ConEd's brazen disregard for the DER Oversight Order all the more egregious is that ConEd *itself* acknowledged that the DER Oversight Order's cybersecurity requirement does not apply to DER Suppliers. It would be one matter if ConEd unintentionally misinterpreted a Commission order. But in this case, ConEd chose to contravene a Commission order knowingly. The Joint Utilities admitted in their Request for Clarification in Case No. 15-M-0180 that "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."[21] The Joint Utilities are correct – the cybersecurity requirement of the DER Oversight Order "specifically does not apply" to GBC registrants.

By assuming presumptuously that the Commission would accommodate the Joint Utilities' desired modifications to a Commission order, and by pre-emptively acting to require executed DSAs of DER Suppliers against the clear direction of the Commission, ConEd has knowingly violated the DER Oversight Order. Mission:data requests that the Commission issue a declaratory ruling that all utilities, including ConEd, must follow the DER Oversight Order and are prohibited from requiring DSAs of DER Suppliers that use GBC unless and until the Commission modifies the UBP-DERS.

6. The DER Oversight Order must be followed, regardless of certain parties' desired modifications to the UBP-DERS.

Some parties argue that the DSAs are appropriate for all DER Suppliers and *should* be required. But that is incorrect when a well-reasoned Commission order based on a lengthy evidentiary, advocacy process resulted in a different conclusion. There is insufficient documentation and policy support for overturning the DER Oversight Order. Commission orders, and the text they contain *as written*, represent lawful instruments of New York State that are binding upon regulated utilities. Mission:data does not seek a declaratory ruling to expand, change or re-interpret the DER Oversight Order. Neither does Mission:data seek a declaratory

---

21 Joint Utilities' Request for Clarification in Case No. 15-M-0180 at p. 2.

ruling on the merits or appropriateness of the DSAs for any entity, ESCO, DER Supplier or otherwise. Instead, Mission:data asks the Commission merely to confirm what it already ordered and require the utilities to act in conformance with such order.

7. The Joint Utilities grossly mischaracterize the cybersecurity risk in demanding changes to the DER Oversight Order.

In their Request for Clarification in Case No. 15-M-0180, the Joint Utilities stated:

> The importance of DERS obtaining and retaining required customer consent before requesting data from the Joint Utilities cannot be understated...Applying the customer data requirements broadly to DERS regardless of the data platform will provide essential protections to customers and Commission oversight over DERS. This is especially important because the DERS-UBPs for most DERS do not call for any Commission registration or vetting process, yet will still require the Joint Utilities to provide highly customer-specific data points to any DERS *and to presume that the DERS properly obtained the customer's consent* [emphasis added].[22]

Nothing could be further from the truth. The GBC standard calls for *the utility* to obtain the customer's consent. GBC makes no "presumption" that DER Suppliers have obtained the customer's consent. In fact, the lack of such a presumption is a *security feature* of the GBC standard that is by design: the customer must grant consent *to the utility* to share his or her data. Does a DER Supplier also receive the customer's consent to receive his or her data via GBC? Yes, of course. But in the GBC standard, the utility does not rely on the *claims* of DER Suppliers that the consent was properly obtained. The customer must provide his or her consent to *both* the utility and the DER Supplier to consummate a GBC transaction. It is precisely that direct, customer-to-utility exchange of consent that makes GBC more secure.

The Joint Utilities' statement is willfully ignorant of the GBC system that the Joint Utilities are in the process of deploying. Worse, the Joint Utilities evidently seek to grossly mischaracterize the severity of the risk in order to unfairly induce Commission agreement with the Joint Utilities' position that the DSAs should be required of DER Suppliers. Mission:data urges the Commission not to be fooled by these inaccurate scare tactics.

---

[22] Joint Utilities' Request for Clarification at p. 2-3.

8. Conclusion.

The Joint Utilities are requiring that DER Suppliers, which receive customer data via Green Button Connect, execute the same DSAs that are used for ESCOs. The DSAs may be appropriate for ESCOs, but the Commission clearly ruled in its DER Oversight Order that they are not applicable to GBC users. Until the Commission amends its prior conclusions, the DER Oversight Order as written is in effect. ConEd is therefore acting not in accordance with the DER Oversight Order, but rather is acting presumptuously as though its desired modifications to the DER Oversight Order have already been adopted by the Commission. Mission:data urges the Commission to issue a declaratory ruling prohibiting any utility from requiring DSAs of DER Suppliers that use GBC unless and until the Commission formally amends the UBP-DERS in this regard.

Respectfully submitted,

for **The Mission:data Coalition**

/s/ Michael Murray

1752 NW Market Street, #1513
Seattle, WA 98107
(510) 910-2281
michael@missiondata.io