NEW YORK STATE
PUBLIC SERVICE COMMISSION

IN THE MATTER OF:

Proceeding on Motion of the Commission to Enable Community Choice Aggregation Programs. — Case 14-M-0224

COMMENTS OF THE MUNICIPAL ELECTRIC AND GAS ALLIANCE
REGARDING THE JOINT UTILITIES' DRAFT DATA SECURITY AGREEMENT

INTRODUCTION

On April 21, 2016, the New York State Public Service Commission ("Commission" or "PSC") issued its Order Authorizing Framework for Community Choice Aggregation Opt-out Program ("CCA Order" or "the Order"), in which it directed all utilities affected by the Order to develop and file a proposed standard Data Security Agreement for Commission consideration. CCA Order, Ordering Clause 5. On June 6, 2016, Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, Niagara Mohawk Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation (collectively, the "Joint Utilities") submitted a "draft Data Security Agreement" to comply with the Order (hereafter "the Agreement" or "DSA"). The Municipal Gas and Electric Alliance ("MEGA") submits these comments on the JU's draft Data Security Agreement.

As a general matter, MEGA supports and endorses the importance of maintaining security of customer information. However, MEGA is concerned that some provisions in the JU's draft Data Security Agreement do not comply with the Order, or are otherwise in need of revision or

clarification in order to ensure that the intent of the Commission in authorizing CCAs is served by these agreements. It is crucial that these security agreements provide for adequate protection of sensitive customer data, but also that the agreements do not unnecessarily complicate or inhibit the development of a CCA in a manner which does not offer any substantive protection to customers. Provisions such as the overbroad and significantly burdensome cyber liability insurance requirements, discussed further below, misunderstand the types of data which will be managed by CCA Administrators and CCA Programs, and results in a misallocation of risk which would serve only to inflate the cost of CCAs, providing no additional data security to consumers. In formulating these comments, MEGA has attempted to identify areas where the draft agreement falls short of providing real consumer protection, and instead creates potential barriers for the implementation or financial feasibility of CCAs.

First, and most significantly, MEGA notes that the draft Data Security Agreement does not properly distinguish between the types of data a CCA Program will need to handle, and which parties involved in the CCA will actually be privy to such data. MEGA submits that not all types of data require security, since they are either already public or relate to aggregate data without individual customer identifications. While MEGA has identified three types of data necessary to implement a CCA Program, only one of these data categories should involve significant security requirements. To the extent that the draft Data Security Agreement fails to distinguish between these data categories, and imposes burdensome or unworkable requirements for less sensitive data categories, it should be revised.

1. Aggregate Data

The first essential category of customer data required for a CCA is actually the least sensitive category of consumer data, since it would require the exchange of no personal or

otherwise sensitive information about any individual customer. Rather, this information would facilitate a CCA Administrator's general understanding of, and planning for, energy consumption needs within a given municipal jurisdiction.

This information is readily available from the utility, but does not identify individual customers. It is aggregated by service class for the whole municipal jurisdiction, and includes, but may not be limited to, total kilowatt hours of energy used, peak load contribution, and number of eligible accounts. These data do not require coverage by the DSA, because they contains no confidential or sensitive consumer information, and the exchange of these data poses no real risk of compromising consumers' confidential or personal information.[1] By contrast, these data are crucial to a CCA Program at an early stage, to facilitate competitive bidding for potential Energy Service Companies (ESCOs) to provide energy supply to the CCA. It would be impossible for a CCA Program to adequately characterize its energy needs without this basic information, but the CCA Administrator would not require the utility to provide it with details at such a granular level that any potentially confidential consumer information would be exchanged. MEGA's proposed CCA Implementation Plan, filed with the Commission on July 7, 2016, sets forth its proposed bid solicitation process, and contemplates requesting only Aggregate Customer Data from utilities at that stage. *See* MEGA Implementation Plan § 8(B).

[1] MEGA acknowledges the point made by the Joint Utilities in this proceeding regarding the potential for a "service class of one," such as a large industrial customer or some other unique service class member or a small number of members, that would essentially be singled out were aggregate data to be released on a service class basis. However, MEGA suggests that, rather than treating all aggregate data as potentially confidential to avoid this problem, the utilities should be permitted to alert a CCA that there exists a service class with only one or a few customer(s), and to suggest that this service class would be combined with another of a similar type when the aggregate data are released, in order to protect the member(s) of the unique service class. For example, a large industrial customer in its own service class could be combined with other large commercial customers, and the aggregate data presented as data for both service classes. MEGA believes that a workable solution to this potential problem could be achieved on a case-by-case basis with utilities or through the adoption of '15/15,' '4/80' or other privacy rules, without the need to expand the scope of the DSA to include aggregate data.

2. Basic/Geographic Customer Data

A CCA Program will also require basic information about the geographic location of potential customers, to verify that those customers are eligible to participate in the CCA Program. This class of information would include only the addresses and customer classifications for consumers within a given municipality. A CCA Administrator will be able to use this information to verify customer eligibility, based on the limitations on CCAs imposed in the CCA Order and accounting for any additional eligibility limitations imposed by a municipality when it adopted a CCA law. But it would not be necessary for the CCA Administrator to have access to these customers' names, their consumption or payment histories, or any other potentially sensitive information about individual customers, since those details would have no bearing on eligibility. This class of information would be compared to existing municipal records, such as tax assessment rolls—which are themselves already publicly available documents and information—to establish eligibility for each potential service account within the CCA's territory. Again, MEGA believes this is already public information by virtue of its counterpart in municipal records, so it should not require coverage by the DSA.

3. Detailed Customer Information

It is only this third class of information which would involve potentially sensitive or personal customer information, and which should fall under the scope of the DSA. The exchange of detailed customer information for the purpose of enrolling and serving customers would require the release of customer names, individual consumption and payment histories, and other permitted categories of personal information necessary to enroll CCA customers with the ESCO that has been awarded the CCA Electric Supply Agreement, and to provide service to those customers. The ESCO would also use this customer list to address and mail the opt-out letters required by the

Commission's CCA Order. The letters will be printed on municipal letterhead provided to the ESCO by the municipality, based on MEGA's Implementation Plan, but the ESCO would be tasked with circulation of these letters to individual customers as part of the obligations set forth in the CCA Supply Agreement.

However, this class of information will be shared *only* between the utility and the selected ESCO—itself a regulated entity subject to the Uniform Business Practices ("UBP") and other Commission rules on consumer protections—and there will be no need for the CCA Administrator or municipality to obtain such detailed personal information. In fact, as suggested in MEGA's Implementation Plan, this detailed customer information should not be shared with the CCA Administrator or the municipality, both because such data are not necessary to enable those entities to perform their role, and because it would create the potential for protected data to be compromised by expanding the scope of individuals and entities with access to such information to include parties who have no practical need for that information. MEGA believes that the guiding principle behind a CCA data security strategy which effectively minimizes risks to consumers should be limiting the scope of shared information, and the circle of persons privy to that information, to only those data which are necessary for each entity to fulfill its obligations, and nothing more.

Therefore, the meaning of "customer-specific data" in the Utilities' DSA should be modified to include only category 3 data, above, but not data from categories 1 or 2. The elements surrounding these definitional approaches will be detailed in MEGA's Data Protection Plan, soon to be filed with the Commission.

Next, the "Authorized Customer-Specific Information" referred to on Page 0, Draft Data Security Agreement, should no longer be required, because the Commission Order (page 50)

suspended relevant provisions of the UBP for municipalities participating in CCA, obviating the requirement of individual authorization for participants to switch to an ESCO.

As noted above, the cyber liability insurance requirement is unnecessary for a CCA Administrator or municipality, given the limited scope of customer information which would be shared with these entities. Under MEGA's proposed model, information about individual customers that would give rise to an insurance requirement will never be handled either by the CCA Administrator, nor any municipality in the aggregations. MEGA's information categorization, and limited sharing process, as outlined above, demonstrates why such a policy is unnecessary. This requirement could prove to be cost-prohibitive, but would offer little in the way of actual protection to consumers, since measures are already being taken to eliminate or minimize these risks.

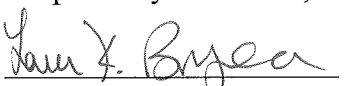
The same is true with regard to the proposed Information Security Program. MEGA believes this requirement would be excessive if imposed on CCA Administrators or municipalities, because the information that would be shared with these entities would not give rise to such a strong need for security. A CCA Program that is designed to limit the scope of information sharing, and the entities with access to information, fulfills the same objectives, but obviates the need for—and costs associated to comply with—this requirement.

On pages 2 and 3 of the DSA, the utilities refer to an "Exhibit A (Vendor Product/Service Security Agreement)" and "Exhibit B (Representative Agreement)" as attachments to the DSA. However, MEGA was not able to locate these exhibits in the Joint Utilities' filings, or elsewhere in this proceeding. MEGA requests that it be afforded the opportunity to review and comment on these exhibits before the Data Security Agreement is finalized.

Lastly, MEGA requests that a revised version of this draft DSA be released for public review and comment before a final agreement is adopted by the Commission and put in place by the utilities. Additional revision of this document will help in ensuring that consumer data are protected, without inhibiting the potential of CCAs to play a new and exciting role in the State's energy future.

Dated: September 12, 2016

Respectfully Submitted,



Laura K. Bomyea, Esq.
Young/Sommer LLC
On Behalf of the Municipal Electric
and Gas Alliance (MEGA)