May 5, 2022

Via E-Filing

Pennsylvania Public Utility Commission,
Attention: Secretary Rosemary Chiavetta
400 North Street
Harrisburg, PA 17120

Docket No. M-2021-3029018
Re: Investigation into Conservation Service Provider and Other Third Party Access to Electric Distribution Company Customer Data

Dear Secretary Chiavetta:

Keystone Energy Efficiency Alliance would like to thank the Pennsylvania Public Utility Commission ("PUC") for this opportunity to provide comments in support of the Conservation Service Provider ("CSP") and Other Third Party Access to Electric Distribution Company ("EDC") Customer Data.

Keystone Energy Efficiency Alliance ("KEEA") is a trade association for the energy efficiency industry in Pennsylvania, which is composed of a diverse range of professions—from contractors and manufacturers to engineers, architects, and software developers—and a local workforce that cannot be outsourced. Together with its sister organization, the Energy Efficiency Alliance of New Jersey ("EEA-NJ"), KEEA represents 75 business members who provide energy efficiency products and services in support of an industry that accounts for more than 65,000 Pennsylvania jobs. Our membership is large and diverse, with experience designing and implementing a variety of demand side management solutions and energy efficiency ("EE") programs across the globe. KEEA champions efficiency as the foundation of a clean, just, and resilient energy economy. KEEA's vision is that energy efficiency anchors all efforts to meet our ongoing energy needs, improve health and comfort, promote energy equity, and protect our climate.

From the 6 questions and 36 subparts outlined by the PUC, KEEA has focused our comments and recommendations on ensuring the expansion of data access to CSP's and other third parties is accessible, secure, and efficient to advance energy savings for Pennsylvanian.

1. Electric Distribution Company (EDC) Smart Meter Customer Data Access by CSPs and Other Third Parties Technical Concerns:

a. Is it possible to develop a path in which certain CSPs or other third parties are granted authorization to access EDC smart meter customer data electronically in a secure manner?

Yes, it is possible to develop a path in which CSPs and other third parties can access customer smart meter data electronically and securely. Several state utility commissions have also explored the topic of third-party access to smart meter customer data and have developed proposed frameworks for secure smart meter data sharing involving Green Button and Green Button Connect ("GB/ GBC").

GB and GBC are the leading data exchange standards for utilities, customers, and third parties to share data in a scalable and uniform manner. Furthermore, these standards should be used fully and are essential for the greatest and widest-reaching impacts throughout Pennsylvania. This is because uniformity leads to the broadest potential for use. To promote its success, regulators should create rules that ensure GBC's standard utility implementation across Pennsylvania to ease access for all consumers and third parties seeking to integrate with utilities' GBC platforms.

g. What criteria should the EDCs utilize to determine eligibility for CSPs and other third parties? Should there be different standards and/or different levels of access to data for different types of CSPs and other third parties?

In determining the criteria for access and what level of access third parties and CSPs have, it is important that the Commission draw a distinction between third parties that provide products and services directly to utility customers, and CSPs or other entities that are providing services on behalf of the utility. While both often interact directly with customers, CSPs have active contracts with the EDCs, making them agents of the utility. This distinction is especially important because EDCs already rigorously vet all CSPs and other contractors before engaging them in the implementation of utility programs, therefore these CSPs and other contractors should not be overburdened with additional technical and IT security requirements that are not already placed upon them by their utility clients. For third parties that are not subject to the same requirements as CSPs, the Commission must instead establish standards that are suitable for third parties who are not agents of the utility to have timely, secure access customer data with customer consent.

h. Should the EDCs require financial security instruments, such as bonds, to help protect data confidentiality? If yes, are rules required to implement these financial security requirements? Also, if yes, should there be different security thresholds required for

different types of CSPs and other third parties? If no financial security should be required, please explain why not.

No. The commission should have the ability to audit the cybersecurity protocols of third parties but not direct the EDCs to require financial security instruments. As previously mentioned, GBC is a data exchange standard that can be used across multiple utilities as it ensures the accessibility of energy usage and billing data in a standardized format that would be auditable by the Commission. Furthermore, EDCs should not be held liable for third party data breaches where the utility customer has consented to the sharing of their smart meter data.

j. How should costs incurred for this purpose be recovered?

The expanded use of data access will create opportunities to modernize utility incentives, especially by incentivizing them to do data-sharing constructively. While EDCs will likely incur additional costs in making customer data more accessible, such expanded access has the potential to also benefit the utility's own demand side management programs and ability to meet their goals under Act 129. Expanded data access benefits all customers by making them the recipients of the cost-savings incurred through programs that benefit from greater data access. Therefore, we recommend that the Commission begin tracking costs associated with expanded data access and consider the option of cost recovery in base rates.

2. EDC Smart Meter Data Access by CSPs and Other Third Parties Legal Concerns:

e. How should a CSP or other third party obtain customer consent for access to data from EDC systems? Would the EDC determine if a CSP or other third party has obtained the proper customer authorization before customer data is provided? If yes, how? If no, please explain why not.

As discussed above, licensed CSP that act as agents of the utility, with contracts governing the exchanges of data, should not be required to obtain additional consent to implement utility programs.

Unlicensed third party requests for customer data can be addressed through the GBC standard, as it is the customer, not the third party, that provides consent to the EDC. This ensures a higher level of privacy and security because the customer is in direct contact with the utility, meaning that the utility does not need to "trust" the third party's claim that a consent is genuine. One key advantage of the GBC approach is that utilities do not need to "police" third parties regarding their consent practices. On the customer's end, the authentication and authorization process (i.e. the consent to share process) should not require greater effort from the customer than what they reasonably use to access their own utility online account.

f. How would the EDC be notified when a customer grants consent for a CSP or other third party to access its' EDC-maintained customer data?

In the case of unlicensed third parties, the EDC does not need to be "notified" of a customer consent because the EDC receives customer consent directly. In other words, there is no separate "notice" process. If the customer does not grant their consent to the EDC, then no data is transmitted.

g. How should a customer withdraw previously granted consent for CSP or other third party access to the EDC's data? How would the EDC be notified of this withdrawal of consent?

For unlicensed third parties, customers should be able to withdraw consent the same way the consent was offered in the first place: via the utility's bill-pay website or by telephone to the utility.

h. How would the EDCs monitor data access to determine if a CSP or other third party becomes a "bad actor" by violating its agreements (failing to maintain data confidentiality, pulling data for a customer without proper authorization, etc.)? What processes could be used to remove access and prevent misuse?

EDCs should not have to police the behavior of third parties and to require them to do so would be improper. Moreover, the utilities should not be liable for a third party's misbehavior, and enforcement of third parties is not a responsibility the utilities want or should have. KEEA recommends that the EDCs' tariffs include the eligibility criteria described above, including the requirement that third parties agree to the DataGuard standard, developed by the United States Department of Energy[1], which is enforceable by state attorneys general and the Federal Trade Commission.

j. Should a utility be held accountable for the improper or illegal acts of a customer-authorized CSP or other third party?

EDCs should not be held liable for third party data breaches where the utility customer has consented to the sharing of their smart meter data and the EDC has no contractual relationship with the third party responsible for the breach.

[1] https://www.smartgrid.gov/data_guard.html

k. What action, if any, can the Commission take against CSPs and other third parties that misuse their access to customer data or the data itself? Please cite to any statutes or regulations that support your answer.

Using the Commission's authority over EDCs, the Commission should order an EDC to terminate access to a third party if the Commission determines that the third party has demonstrated a pattern or practice of breaching the DataGuard privacy standard. Any further punishments by the Commission would violate the Commission's authority as granted to it by the Legislature.

3. Utility Usage Data and Meter Access

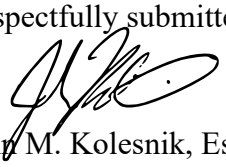
b. What types of data should the EDCs withhold from CSPs and other third parties? Do the EDCs' current systems allow for this data to be restricted?

One of the federal government's Fair Information Practices is the principle of data minimization. In practice, this means that third parties should only be given the minimum information necessary to achieve a customer-authorized purpose. A best practice is for the Commission to explicitly define "unshareable data." At the outset, unshareable data should include bank account numbers, social security numbers, and credit/debit card numbers. Energy management companies do not need such information to render their services, and even if they did, they can ask the customer directly for this information.

Conclusion

KEEA appreciates this opportunity to provide comments on implementation data access to CSP's and Other Third Parties.

Respectfully submitted,



John M. Kolesnik, Esq.
Policy Counsel
Keystone Energy Efficiency Alliance