McNees Wallace & Nurick LLC
100 Pine Street
P.O. Box 1166
Harrisburg, PA 17108-1166

Charis Mincavage
Direct Dial: 717.237.5437
Direct Fax: 717.260.1725
cmincavage@mcneeslaw.com

May 5, 2022

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, PA 17120

VIA ELECTRONIC FILING

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

Dear Secretary Chiavetta:

Attached for filing with the Pennsylvania Public Utility Commission are the Comments of the Pennsylvania Energy Consumer Alliance ("PECA"), Met-Ed Industrial Users Group ("MEIUG"), Penelec Industrial Customer Alliance ("PICA"), Philadelphia Area Industrial Energy Users Group ("PAIEUG"), PP&L Industrial Customer Alliance ("PPLICA"), and West Penn Power Industrial Intervenors ("WPPII") (collectively, "Large Customer Group"), in the above-referenced proceeding.

Sincerely,

Charis Mincavage
MCNEES WALLACE & NURICK LLC

Counsel to the Pennsylvania Energy Consumer Alliance, Met-Ed Industrial Users Group, Penelec Industrial Customer Alliance, Philadelphia Area Industrial Energy Users Group, PP&L Industrial Customer Alliance, and West Penn Power Industrial Intervenors

c:
Jeff McCracken (jmccracken@pa.gov)
Seth A. Mendelsohn, Executive Director (smendelsoh@pa.gov)
Renardo Hicks, Chief Counsel (rehicks@pa.gov)
Dan Mumford, Director, the Office of Competitive Market Oversight (dmumford@pa.gov)
Paul Diskin, Director, Technical Utility Services (pdiskin@pa.gov)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

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

COMMENTS OF THE
PENNSYLVANIA ENERGY CONSUMER ALLIANCE,
MET-ED INDUSTRIAL USERS GROUP,
PENELEC INDUSTRIAL CUSTOMER ALLIANCE,
PHILADELPHIA AREA INDUSTRIAL ENERGY USERS GROUP,
PP&L INDUSTRIAL CUSTOMER ALLIANCE, AND
WEST PENN POWER INDUSTRIAL INTERVENORS

I. INTRODUCTION

On February 8, 2022, the Pennsylvania Public Utility Commission ("Commission" or "PUC") published a Secretarial Letter initiating a proceeding to review the potential avenues for Conservation Service Providers ("CSPs") and other third parties to access Electric Distribution Company ("EDC") customer data. Specifically, the PUC seeks Comments by interested parties to determine if a safe, acceptable path exists for CSPs and other third parties to gain access to customer data electronically from Pennsylvania EDCs. As part of this Secretarial Letter, the PUC provided a list of questions to which interested parties are invited to respond, along with any additional comments or other relevant information to which commenters deem relevant. To that end, interested parties were invited to file comments within 45 days after the date of publication of the Secretarial Letter in the *Pennsylvania Bulletin*.[1]

[1] Pursuant to a request by the Energy Association of Pennsylvania, the PUC extended the date for Comments to May 5, 2022.

Accordingly, the Pennsylvania Energy Consumer Alliance ("PECA"), Met-Ed Industrial Users Group ("MEIUG"), Penelec Industrial Customer Alliance ("PICA"), Philadelphia Area Industrial Energy Users Group ("PAIEUG"), PP&L Industrial Customer Alliance ("PPLICA"), and West Penn Power Industrial Intervenors ("WPPII") (collectively, "Large Customer Group") submit the following Comments responding to the Commission's request for Comments.

II. COMMENTS

A. Introduction

The Large Customer Group is comprised of large commercial and industrial customers with facilities throughout the Commonwealth. The members of these groups use significant amounts of electricity in their manufacturing and operational processes. Moreover, because of the competitive markets in which some members are involved, their usage data is considered sensitive and extremely confidential. As such, the Large Customer Group recognizes that CSPs, as well as some other third parties, may require access to customer usage data; however, because of the sensitive nature of this data, especially of that for large commercial and industrial customers, any entity being provided access to this information must be required to treat this information as such or face ramifications for failing to adequately protect this information.

While allowing CSPs and other third parties access to customer data has the potential to enhance energy services to the benefit of a customer, customer data that is mistreated could not only limit the services provided to the customer, but also have a detrimental effect on the customer's overall business. Thus, before a pathway is provided to make data accessible to any CSP or other third party, the Commission must ensure such pathway provides the adequate protection and parameters needed so that entities receiving this data are held accountable for maintaining the sensitive and confidential nature of such data, as well as providing recourse for customers if such data is abused by the receiving entity.

Similarly, the Commission must recognize that, while CSPs are a narrowly tailored group, allowing access to customer data by any "third party" provides for a wide array of entities that may now or in the future seek to access such data. As such, the Commission must consider the need for parameters around those third parties who should be allowed to access customer data, what requirements must be met before the third party is permitted to access such data, and what control a customer should have over the data available for access. Moreover, because of the broad spectrum of third parties that could seek access to such data, the Commission must consider what ramifications must occur if a third party misuses such data, as well as what remedies a customer has available to it when a third party misuses its data.

Because of the significant and far-reaching issues involved in determining appropriate pathways, the Large Customer Group recommends that the Commission consider convening stakeholder working groups to further evaluate implementation issues. For example, the working groups could consider the parameters around which third parties are eligible to seek access to customer data; the requirements that a CSP or other third party must satisfy in order to obtain such data; the ramifications if a CSP or other third party misuses such data; the remedies available to customers if their data is inappropriately used; the timeframe by which a customer authorization applies; the processes by which a customer can release and revoke authorizations to such data; and the means by which an EDC can verify such authorizations or revocations. By utilizing the findings of such working groups, the Commission can ensure that all issues have been thoroughly addressed and considered prior to implementing a formalized pathway for CSPs and other third parties to access individual customer usage data.

Recognizing, however, that the PUC is seeking responses to specific questions related to these issues, Section II(B), *infra*, provides the Large Customer Group's responses to the questions set forth in the Commission's February 8, 2022, Secretarial Letter.

B. Responses to PUC Questions

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?

The Large Customer Group defers to the EDCs regarding this possibility. Assuming, however, that an electronic pathway would enable an EDC to ensure that the CSP/third party has received adequate customer authorization to access such data, as well as allow the EDC to confirm the customer data each CSP/third party is accessing, the Large Customer Group does not oppose the use of an electronic pathway.

b. Can the web portals available to electric generation suppliers be utilized for this access, or is an alternate pathway necessary?

While the EDCs may be able to provide better insight into this possibility, the Large Customer Group does not oppose the use of web portals available to Electric Generation Suppliers ("EGSs") for access to EDC customer usage data assuming that such web portals would allow EDCs to implement the protocols necessary to protect sensitive customer usage information.

c. Do individual EDCs already maintain an alternative method of data access for CSPs and other third parties? If yes, please explain your system for this access.

The Large Customer Group will defer to EDCs on this question.

d. How are CSPs provided customer data when performing services under ACT 129?

The Large Customer Group will defer to CSPs on this question.

e. What technical limitations currently prevent EDCs from providing smart meter data electronically to CSPs or other third parties?

The Large Customer Group will defer to EDCs on this question.

f. Aside from CSPs, what other third party entities should be considered for potential access?

As noted in Section II(A), *supra*, parameters must be implemented to not only ensure that approved third parties are allowed access to customer data, but also that the PUC has the ability to apply viable remedies in the event a third party mishandles customer data. Certainly, because CSPs are registered entities with the PUC, allowing CSPs to access customer data (with appropriate requirements in place) provides a level of confidence in terms of knowing the entity seeking such information. Conversely, allowing any random third party to seek customer data does not necessarily provide the level of assurance needed in light of the sensitive nature of such data. As such, an overly broad definition of third parties would not be appropriate, but rather, the PUC should consider what parameters can be applied to ensure that third parties seeking customer usage data have suitable reasons for doing so, while also ensuring that the PUC has an appropriate level of review over such third parties.

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?

The Large Customer Group submits that a different level and lower standard could be applied to CSPs or third parties seeking aggregate data. Because aggregate data would not allow an entity to obtain specific customer data, which could be confidential or

sensitive in nature, the standards required to obtain aggregate data need not be as stringent as that for obtaining individual customer usage data. Conversely, individual customer data sought by CSPs and other third parties may contain sensitive customer information, including industrial usage data that if disclosed, could cause competitive harm for the customer. Accordingly, the Commission should provide a separate level of access requiring certain parameters be met, including requiring these entities to comply with any approved opt-in registry, providing customer authorization forms indicating the granting of such information, and holding these CSPs/third parties accountable for any misuse of such customer information.

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.

As noted above, the Large Customer Group submits that an integral part of providing any pathway for CSPs/third party access to individual customer data is the ability for the PUC to apply meaningful consequences to any CSP/third party that misuses or mishandles such data. Requiring CSP/third parties to provide financial security to EDCs would provide a process by which a third party/CSP who misuses customer access data can be penalized. In other words, a suitable consequence for mishandling sensitive customer usage data would be for the third party at fault to lose some or all of its financial security. Thus, requiring third parties to post financial security can incentivize these entities to adhere to the requirements needed to obtain individual customer data, such as obtaining customer authorizations, as well as ensure that CSPs/third parties take the necessary steps to protect such data.

In terms of differing securities for these entities, the Commission should consider setting the financial security based upon the amount of customer data the CSP/third party is seeking. A CSP/third party seeking customer data over a certain threshold should be required to provide additional security so that the security acts as a true incentive for these entities to appropriately obtain and maintain sensitive customer data. Conversely, an entity seeking aggregate data may be permitted to post limited, if any, security, as such an entity would not be receiving sensitive customer usage information.

i. What types of tools should be required to ensure that CSPs and other third parties accessing utility systems have access to help features, such as online trouble ticket systems or technical documentation, to enhance their customer experience? What other features may be necessary?

The Large Customer Group will defer to the CSPs and other third parties on this question.

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

The Large Customer Group does not have a detailed position on the cost recovery process; however, the Large Customer Group submits that cost causation principles require the CSP/third party seeking customer data to pay for any costs incurred for obtaining this data. Requiring customers to bear the costs of such requests would not be just and reasonable, especially if these customers are not the entities for which the CSPs/third parties are seeking data.

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

a. What legal limitations currently prevent EDCs from providing smart meter customer data electronically to CSPs or other third parties?

The Large Customer Group will defer to the EDCs on this question.

b. How do EDCs protect their data when it is provided to CSPs performing services under Act 129 to ensure it is not abused? Can this method be

extended to other CSPs or other third parties not under contract to perform Act 129 services for the EDC?

The Large Customer Group will defer to the EDCs on this question.

c. Could the EDCs utilize contracts to protect the confidentiality of the data? If yes, what limitations currently exist that prevent the utilities from implementing these contracts?

The Large Customer Group will defer to the EDCs on this question, as the Large Customer Group assumes the contract referenced in the question would be between the EDC and the CSP/third party seeking access to data.

d. Would the EDCs need to include any provisions created in these proceedings in a tariff in order to apply them to CSPs and other third parties? What other terms of use should be included?

The Large Customer Group submits that EDCs would need to include any provisions created in this proceeding in a tariff so that the provisions could be properly applied to CSPs and other third parties. A tariff can set forth the specific terms applicable to CSPs and other third parties for accessing customer data, as well as provide parameters regarding what entities are eligible to access such data and the consequences applicable to entities that fail to treat such data as sensitive and confidential.

Terms included in any such tariff should incorporate: (1) the parameters regarding what CSPs/third parties have the ability to access individual customer usage data; (2) the proof a CSP/third party must provide to show that it has met the aforementioned parameters; (3) a standard form obtained by CSPs/third parties to show that the customer for whom the CSP/third party is seeking data has authorized the entity to obtain such data; (4) the process to be used by the CSP/third party to show that the aforementioned form has been obtained; (5) the security requirements that must be met by the CSPs/third parties in order to be obtain individual customer usage data; (6) the clarifications regarding the

consequences that will occur if the CSP or other third party does not maintain the confidentiality of the customer data or if the CSP/third party inappropriately obtains such data; (7) the provisions limiting the timeframe by which a CSP or third party may access an individual customer's usage information, including any renewal requirements; (8) the information regarding how the EDC will inform the customer that its data has been released; and (9) any exemptions to the aforementioned process that would be applicable for an entity seeking aggregate data.

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 not, please explain why not.

The Large Customer Group believes that the most efficient way for a CSP or other third party to obtain customer consent is through a standardized form to be used by all third parties to confirm that a customer has agreed to allow the third party to access its data. The standardized form should also include the timeframe for which the customer is permitting the third party to access this individual customer data. This standardized form should be included as part of any request by a third party seeking to obtain individual customer usage.

The Large Customer Group submits that a signed customer authorization form must be provided to the EDC before the release of any data; however, if this requirement is not applied, then, at a minimum, the third party should be required to maintain copies of all such authorization forms that can be produced upon the request of the EDC or the customer. Importantly, if the third party cannot produce such form upon request, provisions should be in place that would result in repercussions to the third party, including restrictions from obtaining any individual customer data from any EDC in Pennsylvania and remedies for the customers whose data has been mistreated.

Additionally, the customer authorization process should include a process through which customers, or at minimum large Industrial customers, must affirmatively opt-in for any EDC provision of individual customer data to third parties. The Commission could consider centrally maintaining the opt-in registry similar to the manner in which the Pennsylvania Attorney General's office maintains the "Do Not Call" registry for customers opting out of telemarketing communications. Opting-in to the registry would supersede any other form of customer authorization, meaning that a subsequent customer authorization received by an EDC from a third party would be declined for any customer listed on the registry. However, customer authorizations would still be required for those customers that have not opted-in to the registry. As a result, the registry does not replace the customer authorization process, but rather provides a second layer of customer protection against inadvertent EDC disclosures arising from errors or miscommunication related to the customer authorizations.

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?

As noted above, the third party seeking access to individual customer data should be required to provide a signed authorization form to the EDC prior to the EDC releasing such information. The Large Customer Group would be interested in reviewing the EDCs' position on this issue, but, initially, the Large Customer Group believes that a web portal, similar to that currently utilized and managed by EDCs for EGS access to data, may be a viable tool by which the third party could post its customer authorization forms for confirmation by the EDC.

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?

As discussed above, the Large Customer Group strongly supports the EDC notifying a customer when a third party has requested access to the customer's individual usage data. This initial step provides the customer an immediate opportunity to object if authorization was not provided. On a going forward basis, the EDC should have a provision in its tariff that would allow the customer to indicate to the EDC that consent for a third party to access its data has been withdrawn. The Large Customer Group would seek insight from the EDCs as to the best means by which to indicate such withdrawal, be it an email or a form revoking such authorization.

In addition, any authorization should be for a limited time, such as one year with any renewal subject to an updated customer authorization. Providing such boundaries regarding authorizations will help to eliminate the need for revocations of authorizations over a long-term basis. Moreover, a customer may enter into a contract with a CSP or other third party for a limited period of time (*e.g.*, two years), but after that timeframe, the customer may choose to not renew that contract and instead seek the services of a different CSP/third party. Placing a limited timeframe on the authorizations will ensure that a third party with whom a customer is no longer contracting will not have the ability to continue to review that customer's sensitive usage data.

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?

In order for EDCs to monitor the activity of CSPs or other third parties to determine bad actors, the EDCs should be required to conduct regular, quarterly, randomized audits

for at least 10% of the active third parties governed by the tariff. "Bad acting" should include, but not be limited to, failing to maintain data confidentiality, obtaining customer data without proper authorization, lacking appropriate documentation regarding customer authorization, or failing to appropriately treat usage data as confidential. As noted previously, if a third party becomes a "bad actor," the third party should be barred from obtaining access for customer data from any EDC in the Commonwealth, as well as forfeiting any security that the third party provided in order to be eligible to access such data.

i. For third parties that serve as both a Distributed Energy Resource Aggregator under FERC Order 2222[2] and a CSP, what limitations on the use of data should be placed on them to prevent unauthorized use between roles?

The Large Users Group does not have a position on this issue at this time.

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

Assuming no negligence or willful misconduct by the EDC and that the EDC has followed all PUC established protocols for allowing a third party to obtain individual customer usage data, including confirming authorization by the customer and conducting regular audits, the EDC should not be held accountable for the improper or illegal acts of a third party.

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.

Pursuant to 52 Pa. Code Section 54.8, neither an EDC nor an EGS may release private customer information, including a customer's historical billing data, to a third party

[2] Available at https://ferc.gov/sites/default/files/2020-09/E-1_0.pdf.

unless the customer has been notified of the intent and has been given a convenient method of notifying the EDC/EGS of the customer's desire to restrict the release of private information. 52 Pa. Code Section 54.8(a)(2).

Using this provision as a baseline, any third party access to customer billing data must first require that: (1) the customer has been notified of the request; and (2) the customer has been given a method to restrict the release of such sensitive data by an EDC/EGS. As noted herein, the Large Customer Group supports a requirement that EDCs alert customers when a third party is seeking usage data in order to ensure that the customer intends for such highly sensitive data to be released. Requiring such notification comports with Section 52 Pa. Code Section 54.8(a). Moreover, having a basis by which the customer may restrict the release of billing data, combined with the requirement that third parties seeking such data must provide an authorization from a customer who has not restricted release provides an added layer of protection to ensure that a customer's confidential data is treated as such. *See* 52 Pa. Code Section 54.8(a)(1).

If, however, a third party mishandles such information, the PUC must have a method by which to reprimand the faulty third party. For these reasons, the Large Customer Group recommends that a third party who mishandles sensitive customer information should be prohibited on a going forward basis from accessing customer data from any EDC in the Commonwealth. Moreover, the Large Customer Group supports requiring third parties seeking such data to post security with the EDC. For any third party that misuses such data, the third party should forfeit its posted security. The PUC should also consider what remediation can and should be provided to any customer whose sensitive data has been mishandled.

For example, if an industrial customer's sensitive usage information is mishandled, the industrial customer would need to consider seeking relief from the court of common pleas. Requiring a customer to bear the burden of obtaining such relief, inclusive of court costs, due to the mishandling of confidential information by a third party is unjust and unreasonable. Thus, the Commission must ensure adequate levels of protection are in place, especially for industrial customers, prior to an EDC releasing such information. Moreover, the Commission should consider what relief can be provided to a mistreated customer who, through no fault of its own, has no ability to put the "genie back in the bottle" after sensitive data is mishandled.

3. Utility Usage Data and Meter Access:

a. What customer data should the utility share with CSPs and other third parties? Should different types of CSPs and other third parties have different access to customer data?

The Large Customer Group would seek additional insight from CSPs and other third parties participating in this proceeding regarding the data they would be seeking beyond individual customer usage data. With that said, if the CSPs and other third parties are merely seeking aggregate data, the parameters regarding financial security and customer authorizations need not apply, as sensitive data would not be released under these circumstances.

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?

As noted above, the type of data that should be withheld from CSPs and third parties would depend upon whether the CSPs and third parties are seeking individual customer usage data or aggregate data, as well as whether the CSPs and third parties have met the requirements for individual customer usage data if that is the information requested. We

will defer to EDCs regarding whether a system is currently in place that allows for this data to be restricted.

c. In what format should the data be given? Should the data from each EDC be in an identical format (similar to the Electronic Data Exchange Working Group web portal data)? What other technical standards should be applied to the data?

The Large Customer Group will defer to EDCs on this question.

d. Should aggregated data (i.e. – benchmarking or geographic data) be made available? Should aggregated data be available to a wider array of CSPs and other third parties?

The Large Customer Group does not oppose aggregate data being made available to a wider array of CSPs and other third parties, assuming such data is genuinely "aggregate" and does not contain specific customer information, such as load usage or other sensitive information.

e. Should the Commission establish standard protocols and communication mediums for providing direct access to usage information from the meter to the Home Area Network? If so, what should those be?

The Large Customer Group does not have a position on this question at this time.

f. Should CSPs and other third parties be provided direct access to the meter? What policies or regulations should this Commission promulgate to ensure that these CSPs and other third parties are provided timely access under reasonable terms and conditions to the EDC's customer metering facilities?

The Large Customer Group opposes allowing CSPs and other third parties direct meter access, as such access seems beyond the scope of information needed by CSPs and third parties. Moreover, for many large industrial customers, meter data is located inside of the fence line and tied into the customer's network. Thus, allowing third parties access to a customer's meter may present a security risk for the customer that would need to be

addressed, such as providing a smart meter data file that is secure from access to the smart meter itself.

g. What communications, software, or hardware can facilitate this direct access to the meter for customers and their approved CSPs and other third parties, and should the Commission establish requirements and or standards to facilitate this access?

As noted above, the Large Customer Group opposes allowing CSPs and other third parties access to industrial customer meters, especially if such access does not address the security risks that could be prevalent for industrial customers. Moreover, if the PUC implements the Large Customer Group's suggestion to provide a smart meter data file that is secure from access to the smart meter (in order to address security risks), the EDC would need to be responsible to ensure that the meter data has been reviewed and "cleaned" prior to providing this data to a third party. The Large Customer Group has found that communication issues, meter failures, etc., may impact meter data. As a result, such data must be reviewed prior to presenting to a third party to ensure that "bad" data is not provided, which would result in a misrepresentation of a customer's load.

h. What electronic access to customer meter data do CSPs, other third parties, and EGSs need from EDCs, that they currently do not have? Provide specific examples where these entities do not have such access currently, and provide examples, if available, of electronic transactions that can be adopted to facilitate access.

The Large Customer Group will defer to CSPs and third parties on this question.

4. Home Area Network (HAN) Protocols:

The Large Customer Group does not have a position on Home Area Network protocols at this time.

5. Automatic Control:

a. How can smart meters "effectively support" automatic control of a customer's electricity consumption by customers, utilities, and the customer's CSPs or other third parties.

The Large Customer Group would prefer to review the EDCs and third party responses on this issue prior to commenting.

b. How is the smart metering system engaged in the initiation, maintenance, relinquishment, and verification of the automatic control of customer consumption?

The Large Customer Group will defer to EDCs on this question.

c. What smart metering protocols and communication meters are needed to implement these automated controls? Should the Commission establish standard protocols and standards for this purpose?

The Large Customer Group will defer to EDCs on this question.

d. What energy consumption customer asset can be controlled by these smart meter system for each of the customer segments, and how is control of these assets impacted by the choice of communication medium and protocol?

The Large Customer Group will defer to EDCs on this question.

III. CONCLUSION

WHEREFORE, Pennsylvania Energy Consumer Alliance, Met-Ed Industrial Users Group, Penelec Industrial Customer Alliance, Philadelphia Area Industrial Energy Users Group, PP&L Industrial Customer Alliance, and West Penn Power Industrial Intervenors respectfully request that the Pennsylvania Public Utility Commission consider these Comments in evaluating potential avenues for Conservation Service Providers and third parties to access Electric Distribution Company customer data.

By 

Susan E. Bruce (Attorney I.D. #80146)
Charis Mincavage (Attorney I.D. #82039)
Adeolu A. Bakare (Attorney I.D. #208541)
McNees Wallace & Nurick LLC
100 Pine Street
Harrisburg, PA 17108-1166
Phone: 717.232.8000
Fax: 717.237.5300
sbruce@mcneeslaw.com
cmincavage@mcneeslaw.com
abakare@mcneeslaw.com

Counsel to the
Pennsylvania Energy Consumer Alliance,
Met-Ed Industrial Users Group,
Penelec Industrial Customer Alliance,
Philadelphia Area Industrial Energy Users Group,
PP&L Industrial Customer Alliance, and
West Penn Power Industrial Intervenors

May 5, 2022