The Citizens Utility Board of Michigan is pleased to submit several suggestions to further improve the Staff's Data Access and Privacy Recommendations.

Access to customer data is a sensitive subject because while the opportunities that come with more open data access are potentially huge, dangers like identity theft and invasions of privacy loom. The Staff's recommendations for the most part strike the right balance between the priorities of keeping the door open for those opportunities and maintaining customer safeguards to ward against those dangers. CUB offers several more recommendations that can hopefully further enrich the Staff's recommendations.

First, the staff should use more specific language to make clear that customer data should be kept safe from particularly invasive uses by third parties. A common example is the reselling of data by third parties for purposes of advertising. While the Staff wisely recommends that sensitive data be anonymized and/or only available at customer discretion, even if a customer consents to data being shared by utilities with third parties, there should be the option for the customer to make clear that that consent is conditional on the third party not reselling or otherwise distributing data to fourth, fifth, etc. parties.

Second, low-income customer needs merit additional consideration. We fully support the Staff's recommendation that the utilities pilot home area network technology to provide other options for low-income and vulnerable populations who may have limited access to the Internet to view and control their data. CUB adds that such technologies should be provided at no charge to customers in these groups. There are examples of other states, such as Texas, that have provided free at-home monitors for low-income customers to help them view AMI data.[1]

Finally, the recommendations should also tackle the important practical issue of the means by which a customer authorizes third-party data access. The act of authorization should be a clear, active step by the customer, and not a situation where, say, the customer fails to check a box on an online form and as a result gives up his or her data. Requiring verbal consent by telephone or written consent from the customer via email or letters may be the strongest examples of active steps by customers that would unambiguously register their authorization.

Requiring that high bar for all third-party applications may be too burdensome, however. For example, since the MPSC appears to be recommending Green Button Connect to be the main "portal" a customer uses to access their data, it would not be practical or desirable to force a

[1] See: "For example, the Public Utility Commission of Texas has approved both consumer-education efforts related to Smart-Grid and the funding of a program that will provide low-income consumers with free in-home monitors to help them monitor their energy uses." U.S. Department of Energy. "Data Access and Privacy Issues Related to Smart Grid Technologies." October 2010. https://www.energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf

customer to jump through hoops to begin using this portal. Instead, the MPSC and stakeholders should consider what third party applications may need to have additional levels of customer consent to access their data and which may not.

Thank you for the opportunity to comment.