



September 30, 2022

Secretary of the Board
New Jersey Board of Public Utilities
44 South Clinton Avenue, 1st floor
Trenton, New Jersey 08625

RE: Comments of Mission:data Coalition on Docket No. EO20110716 regarding Draft Minimum Filing Requirements for Advanced Metering Infrastructure Plans

To Whom It May Concern:

Mission:data Coalition (“Mission:data”) is pleased to provide these comments in response to the Board of Public Utilities (“Board” or “BPU”) July 29, 2022 notice seeking stakeholder input on the Draft Minimum Filing Requirements (“Draft MFRs”) regarding Advanced Metering Infrastructure (“AMI”) Data Transparency, Privacy & Billing (the “Straw Proposal”) in the above-referenced docket. Mission:data provides recommendations based upon the discussion items that arose during the two technical sessions (August 16, 2022 and September 6, 2022), as well as general comments regarding the Draft MFRs. Our recommendations below are intended to supplement our detailed written comments provided on October 7, 2022.

By way of background, Mission:data is a national non-profit coalition of 30 technology companies across North America delivering data-enabled services that focus on providing direct energy and carbon savings to all utility consumers (residential, commercial, industrial and institutional customers). These services range from detailed energy usage analysis and energy feedback technologies to demand response, electricity commodity supply, and device control. Our members are the leading innovators in the energy management industry, representing over \$1 billion per year in sales. We have been active in 15 states across the U.S. helping to craft data access policies. For more information, please visit www.missiondata.io.

Mission:data believes all consumers should have convenient access to the best available information about their energy usage and costs, and the ability to share that data with any third party of their choice. Today, some five states (California, Colorado, Illinois, New York and Texas) have required their utilities to provide “energy data portability,” meaning the ability for consumers to share their energy information held by electric and gas utilities with non-utility service providers, covering over 36 million electric meters. Some of these third party providers include smartphone apps that help consumers save energy by analyzing their usage patterns with new software tools; some provide heating, ventilating and air conditioning controls that maximize comfort while providing load-shedding capabilities to the grid; and some provide commercial and industrial demand response offerings. Mission:data advocates for technologically consistent, open standards for sharing energy data across jurisdictions.

Recommendations of Mission:data Coalition

1. **The Minimum Filing Requirements (MFRs) should require timely access to unvalidated usage data that is “backhauled,” i.e. sent from the meter to the utility and then to a customer-authorized third party, prior to being deemed “billing quality.”** Mission:data applauds the Draft MFRs for considering both validated usage data and unvalidated usage data in Section 2, “AMI Data Provision Timelines.” However, we believe that the scope of unvalidated usage data should be expanded, as explained below. With regard to unvalidated usage data, the Draft MFRs say only that such information should be shareable “with home area networks where feasible.” Mission:data believes this is inconsistent with other jurisdictions and would inadvertently reduce the value of AMI to consumers. The solution is for electric distribution companies (“EDCs”) to provide, via their Green Button Connect (“GBC”) platforms, an automated way to access unvalidated usage data *prior* to waiting 48 hours. Let us explain how the process works in other jurisdictions and how the current gap in the Draft MFRs can be resolved. Most utility billing systems complete the validation, editing and estimation (“VEE”) process after 24-48 hours, at which point “billing quality” usage data is finalized and ready for transfer to third party energy management firms. Mission:data strongly supports requiring EDCs to deliver validated data via a standards-compliant GBC platform. However, there is significant additional value to ratepayers if customer-authorized entities are able to access “raw,” unvalidated usage data via the same GBC system – without having to rely on the Home Area Network (“HAN”) – on a timeline sooner than 24-48 hours. Mission:data notes that several utilities nationwide support near-real-time provision of raw usage data via GBC – for example, Consolidated Edison in New York allows customer-authorized entities to request raw usage data via a GBC system with only a 15-minute or 30-minute lag time, which is far superior to a 24-48 hour lag time. Lower latencies can drive significant value for demand reductions; indeed, notifying a commercial customer that they are exceeding their all-time monthly peak some 48 hours after the event occurs is not helpful for taking timely action. And as acknowledged in the Draft MFRs, the HAN is not feasible for many customers due to range limitations. Thus, while Mission:data strongly supports the HAN, an optimal solution is for EDCs to be required to provide raw, unvalidated usage data as promptly as possible – taking into account the differences of each EDC’s AMI system latencies – *in addition to* providing bill-quality readings once available. Mission:data notes that energy management firms understand and can accommodate the occasional incorrect reading that may occur; the value of timeliness to energy management services far outweighs the occasional erroneous value. Finally, the Green Button standard is designed to accommodate the transmission of updated usage values over time using a “flag” for each interval usage data point known as “QualityOfReading,” and so Mission:data’s recommendation is entirely consistent with the technical standard.
2. **The requirement for multi-factor authentication should be replaced with a policy of symmetrical authentication practices regardless of the activity.** Mission:data is concerned that support for multi-factor authentication (“MFA”) among utilities nationwide varies widely. Requiring EDCs to require MFA of customers wishing to share their energy information but *not* requiring MFA for some New Jersey customers to merely pay their bills online would be to erect an arbitrary and unfair barrier that will inhibit customers taking advantage of energy management services. A better solution is to have a level playing field in which utility authentication practices, whether MFA or not, should apply universally to customers regardless of the activity. Today, many customers can – without MFA – log into their EDC’s website and start and stop electric service. It would be foolish to establish a “lighter” authentication

standard for stopping electric service – a potentially high-risk action that could render medical equipment inoperable or turn off heating systems during dangerous cold weather – and a “stricter” authentication standard, MFA, for a relatively low-risk action such as sharing data with an energy management provider. The solution is for the Board to avoid the specificity of MFA in the MFRs altogether and simply require symmetry between the authentication practices of all online transactions: Whether a customer wishes to pay a bill, start or stop service, sign up for bill alerts, or share their energy data with an energy management provider, the authentication requirements should be identical in each case. If an EDC believes it is reasonable and necessary to require MFA for all online transactions, then it can do so, provided that MFA is universally required. If an EDC does not believe MFA is reasonable or sufficiently mature for all online transactions, then MFA should not be required for any online activity.

3. **NIST standards should clearly specified, and they should apply to EDCs, not to customer-authorized third parties.** During the technical sessions, Staff proposed that EDCs and customer-authorized third parties would be required to adhere to “NIST standards” with regard to cybersecurity. Mission:data wishes to make two points on this topic. First, the Board’s jurisdiction is limited to regulated utilities, and so establishing requirements for energy management firms that are not regulated and do not provide electric service would exceed the Board’s authority. Mission:data wishes to put the Board at ease on this issue. Many states – such as California, Colorado, Illinois – have successfully established GBC platforms despite state commissions lacking authority over customer-authorized third parties. The risk of a third party experiencing a cybersecurity issue and somehow “infecting” EDCs is extremely low because customers must grant their consent before third parties can access **any** data from the EDC. It is up to the EDC to provide **only** the information authorized and nothing more. If an “infection” of an EDC were to occur as a result of a third party, such a remote eventuality could only occur if the EDC had not properly managed its own security.¹ Second, if the Board wishes to require EDCs to follow NIST standards, then we encourage the Board to define **which** specific NIST standards it is referring to and how compliance will be evaluated. There are literally thousands of NIST standards ranging from narrowly-focused authentication practices to broad cybersecurity frameworks and guidance documents, and everything in between. Many NIST “standards” are actually conceptual outlines, and thus evaluation of adherence may be inherently subjective. If the Board wishes to impose any cybersecurity standard beyond merely “reasonable cybersecurity practices and procedures,” then the Board must be more specific.
4. **The Board should avoid putting EDCs in the role of “policemen” over customer-authorized third parties.** The Draft MFRs state that “EDCs [shall] maintain a ‘bad actor’ list of third-party entities that are banned from participation in AMI data sharing...” Mission:data urges the Board to reconsider, because the Draft MFRs would put the EDCs in the role of investigators and enforcers against their perceived competitors – energy management firms. Not only is this role inappropriate and a conflict of interest for EDCs, but EDCs do not want this role, either. Mission:data’s experience in other jurisdictions is that appointing – explicitly or implicitly – the

¹ An example from another industry is Stripe, the global online payments company. Stripe allows merchants to write software into their website storefronts in order to process credit card payments. Merchants could, in theory, write malicious code that fraudulently steals credit card numbers; however, this is impossible in practice because Stripe has built its application programming interfaces to prevent this type of attack. Thus, Stripe does not conduct cybersecurity audits of merchants prior to integrating their systems together. Similarly, the Board can ensure adequate cybersecurity of the electric system through its oversight of EDCs alone, without resorting to extra-jurisdictional requirements on third parties.

EDCs as policemen will inevitably lead to customers being deprived of value from AMI. Simply put, utilities are extremely risk-averse and will inevitably reduce or eliminate data-sharing because it presents risks without financial rewards to EDCs. The solution is to amend the Draft MFRs to include the following enforcement process that better respects due process and avoids conflicts of interest, as further explained in our October 7, 2021 comments. The BPU, not the EDCs, must maintain the list of “banned” third parties. Third parties can only be added to the “banned” list after a Staff investigation and allowing for due process. EDCs cannot unilaterally terminate access to a particular third party without a Board order.

5. **Proposed additional data fields should be re-examined.** The Draft MFRs call for three additional data types to be provided: (1) “AMI Data to track electric vehicle charging,” (2) the identification of premises as disadvantaged communities, and (3) the potential use of AMI data for future volt/VAR services. Mission:data supports Staff’s intentions here but believes that (1) and (2) should be further clarified via workshops prior to being required. For most energy management firms, they already have ready access to geographic databases from the state or federal government regarding income, air quality and proximity to polluted or contaminated sites; EDCs are not equipped to be the conduit for this information. Furthermore, “tracking electric vehicle charging” is unclear, and this may be better addressed through meter-based “apps” as described in Section 7 of the Draft MFRs. For these reasons, (1) and (2) should be removed.

Finally, we strongly encourage the Board to reconsider our detailed comments from October 7, 2021 – in particular, our recommendation for a hosted, centralized repository of energy data in order to provide “one stop shopping” for customers and for energy management firms. A centralized system is the only way to achieve maximum efficiency and reduce friction and transaction costs. Texas was the first state to provide a single web portal for retailers and third parties to access customer information called Smart Meter Texas (“SMT”). The objective was to provide a central clearinghouse of advanced metering data across the state’s four large distribution utilities, making it much easier for third parties to get the information they need. Similar efforts in other states such as New Hampshire and New York are underway. We strongly support a requirement in the MFRs for the utilities to, at minimum, investigate the feasibility of a centralized repository for New Jersey.

Thank you for the opportunity to provide comments.

Sincerely,

_____/s/_____
Michael Murray, President
Mission:data Coalition
1752 NW Market Street #1513
Seattle, WA 98107
michael@missiondata.io
(510) 910-2281