c/o 25 Corporate Drive, Suite 103
Burlington, Massachusetts 01803

June 20, 2011

North American Energy Standards Board
c/o Jonathan Booe, Deputy Director
801 Travis, Suite 1675
Houston, Texas 77002

Submitted by email to: naesb@naesb.org

Re: Comments on R10012, Retail Electric Quadrant Data Privacy Task Force on Third Party Access to Smart Meter-Based Information

This is a comment in response to the request for comments on the North American Energy Standards Board (NAESB) Retail Electric Quadrant (REQ) Data Privacy Task Force recommendations (R10008) on Third Party Access to Smart Meter-Based Information. I have served as an active participant in the US federal SmartGrid Interoperability Panel (SGIP) substantive standards panels whose work is affected by the proposed recommendations, including its PAP10 smart meter information panel, and the SGIP CSWG Privacy committee's subcommittee on third party rights.

For identification purposes, I currently serve as the general counsel and previously was the director of standards of OASIS, one of the open standards consortia contributing to the SGIP program; and prior to that, served as as general counsel to a health care informatics consultancy providing expert HIPAA privacy advisory and technical services. However, please note, the following comments are personal views, submitted as a participating expert for the general improvement of the proposals, and not representing the position of my employer or any other entity.

1. Coordination with ESPI

Separately I have offered comments to NAESB's draft R10012 Energy Services Provider Interface being produced by the Energy Services Provider Interface Task Force. That draft document, for which informal review has recently closed, describes a technical interface for transactions conveying certain Retail Customer meter data under the initial control of Distribution Companies to Third Parties (as defined in ESPI).

As this draft recommendation (R10008) addresses best practices associated generally with the same set of information flows and use cases as the ESPI interface document (R10012), it would be helpful to implementers if the defined terms used in both documents (e.g., Distribution Company, Third Party, etc.) are aligned where logically possible.

However, I note that because ESPI is a voluntary interface profile, not all entities in a defined class (such as 'Distribution Company') may use the interface. So defined classes in the ESPI document that refer only to those who implement that interface will be subsets of, and *not identical* to, some defined classes of entity in this (R10008) document. This is because a general practice described as beneficial in this R10008 recommendation (for example, Third Parties *should* take certain steps to train their employees handling Retail Customer data) likely would apply to both those third party meter data recipients who do, and who do not, participate in R10012 ESPI exchanges. So definitions that are limited to ESPI users in the R10012 documents may not serve well in the R10008 documents.

See also the concern about “Data Custodians” as a separate class, below.

2. Distinctions between “Third Parties” as defined in R10008 and “contracted agents”.

I am concerned that the general topic of this (R10008) recommendation, which addresses the sharing of potentially-private Retail Customer data by Distribution Companies with other, separate entities, may artificially distinguish between (a) “Third Parties” who seek customer data on their own initiative, or that of the customer, on the one hand, and (b) parties who use customer data at the behest of the Distribution Companies, which may include “contracted agents”, and perhaps also the type of entity described as “Data Custodian” in the ESPI (R10012) documentation.

2(a) Are Data Custodians contracted agents?

Among other things, it may be helpful to confirm whether all parties who may serve as a Data Custodian, in the ESPI R10012 sense, necessarily are “contracted agents.” If not, then they might be a third hybrid class of meter data consumer, as to which this recommendation is accidentally silent.

2(b) Do contracted agents have any need for privacy practices relevant to this document?

As pointed out by the R10008 comments recently submitted by the American Public Power Association, this task force constrained itself to assume that pre-existing “Applicable Regulatory Authorities” and “Governing Documents”, as in place for utilities today, provide adequate privacy protection to retail customers.

The proposed recommendation extends that assumption all “contracted agents”, who are included within the expanded class of “Distribution Companies”, and excluded from the definition of “Third Parties” for which some best practices are offered. As I understand it, the underlying assumption is that such agents are acting on behalf of and at the direction of regulated Distribution Companies, and that, therefore, the agents' operations involving potentially private customer data need no treatment in this document, as they are fully addressed by Governing Documents and Applicable Regulatory Authority.

I note that the definition of “Governing Documents” includes (in addition to legal mandates) the existing body of operating manuals and service contracts in use by Distribution Companies. So, the proposed recommendation essentially elects to leave alone, and to make no evaluative judgments or recommendations about, any privacy behaviors or breaches of contracted agents, or guidance or practices regarding them.

This is a significantly different approach from the “Business Associate” rules promulgated under the US HIPAA and HITECH regulations, governing certain types of personal and private information exchanged in health care and health payment transactions. See. e.g., Section 164.502(e)(1) of the HIPAA Privacy Rule promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (in which the regulated entities are required to obtain “satisfactory assurance” that the nonregulated recipient entities – “business associates” – will “appropriately safeguard” private information), and Section 13408 of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

There undoubtably will be privacy risks and issues in contracted agent operations on meter data, whether or not those activities are addressed by this recommendation. The newly highly networked nature of electronic exchanges of customer meter data, as contemplated by the SmartGrid program, appear likely to create as many novel and increased opportunities for data loss, breach and

inadvertent disclosure by newly-emerging types of “contracted agents”, in complex data exchange and data brokering business models, as by non-agent “Third Parties”.

While there is nothing logically wrong with this task force's initial decision to leave all privacy operations of contracted agents unexamined, as a community, we will need to be clear that R10012 is not offered as a solution or answer to any questions about those operations.

3. Exceptions to the general theme of addressing only Third Party exchanges

In view of the foregoing exclusions, it seems possible that other stakeholders will at some future point offer or recommend various common privacy practices for application to Distribution Companies and their contracted agents. I did note that there are some parts of this proposed recommendation that appear to recommend practices to Distribution Companies, without any reference to Third Party data exchanges. E.g.,

- At lines 231-233, certain recommended practices regarding terminated employees;
- At lines 451-454, certain recommended practices regarding sharing of data as between current versus prior residential address occupants;
- At lines 460-467, certain recommended practices regarding disclosure upon receipt of legal process; and
- At lines 532-539, certain recommended practices regarding notifications to customers of privacy breach.

While these may be good recommendations in context, their presence as general guidance to Distribution Companies somewhat undermines the theory that this recommendation gives no general advice. If these tenets are considered necessary as general recommendations – above and beyond what is presently supplied by Applicable Regulatory Authority and Governing Documents – the question may be raised whether they are a sufficient or complete set, or whether the pre-existing rules have been analyzed and found in need of augmentation in those areas only.

Thank you as always for your consideration and open process.

Respectfully submitted,

/s/ JBC

James Bryce Clark

cc: Rae McQuade, President, NAESB