

**ICC Docket No. 14-0507**

**Commonwealth Edison Company's Response to  
Illinois Commerce Commissioners' Data Requests**

**ICC 1.01-1.02**

**Date Received: October 16, 2014**

**Date Served: November 6, 2014**

**REQUEST NO. ICC 1.01:**

To the best of your ability, please provide a comprehensive list of States whose Public Utility Commissions, or equivalent regulatory authority, have specifically addressed any one or all of the following issues within the context of smart meter or smart grid implementation: data ownership, types of data, third-party access to data, data formats, methods of delivering data, timeliness of data delivery, quality of data, data security, the use of national standards, and whether or not charges should be assessed for accessing data.

- a. Please describe the issue(s), the manner of proceeding in which the issue was addressed and the date that the issue was resolved. Please also provide an explanation of how the State Commission or equivalent regulatory authority resolved the issue(s).

**RESPONSE:**

Please see the attachment labeled as ICC 1.01\_Attach 1 for a chart listing regulatory proceedings in seven (7) States addressing smart meter data practices and rules based on research conducted to the best of Commonwealth Edison Company's ("ComEd") ability given the time constraint for responding. The attachment labeled as ICC 1.01\_Attach 1 is not meant to be an exhaustive list of all state jurisdictions that may have addressed the issues set forth in the Commissioners' Data Request ICC 1.01.

State	Proceeding	Issues Addressed	Date Resolved	Finding(s)
California	California Public Utilities Commission Decision 11-07-056	<ul style="list-style-type: none"> <li>Data security</li> <li>Third party access</li> </ul>	7/28/2011	<p>Adopted “Rules Regarding Privacy and Security Protections for Energy Usage Data” based on the Fair Information Practice Principles.</p> <p>Utilities must provide customers with notice of what data is collected and for what purpose the data is used on a yearly basis via the utilities’ homepage, with links sent to customers on all emails.</p> <p>Customer has ability to access usage information.</p> <p>Third parties should only get data necessary to accomplish the primary purpose and should not hold onto data longer than reasonably necessary.</p> <p>Customers must be notified in event of breach.</p> <p>Utility must perform periodic audits of privacy and security practices.</p>
	California Public Utilities Commission Decision 13-09-025	<ul style="list-style-type: none"> <li>Third party access</li> </ul>	9/19/2013	<p>Adopted a process for oversight of third parties receiving customer data from the utility.</p> <p>In order for third party to obtain usage information, the third party must show:</p> <ol style="list-style-type: none"> <li>(1) third party has obtained customer’s authorization;</li> <li>(2) third party meets technical requirements;</li> <li>(3) acknowledge receipt of utility tariffs and applicable rules; and</li> <li>(4) are not otherwise prohibited by the CPUC from receiving such information.</li> </ol> <p>Adopted a customer information service request form for parties seeking only usage information.</p>
	California Public Utilities	<ul style="list-style-type: none"> <li>Third party</li> </ul>	5/5/2014	Adopted rules that provide access to energy usage and usage-

<p>Commission Decision 14-05-016</p>	<p>access</p> <ul style="list-style-type: none"> <li>• Data formats</li> <li>• Timeliness of data delivery</li> <li>• Methods of delivering data</li> </ul>	<p>related data to local government entities, researchers, and state and federal agencies.</p> <p>Formed Energy Access Data Committee to advise the utilities on process improvements and best practices related to data access and help mediate disagreements between the utilities and data requesters.</p> <p>Utilities must post certain aggregated monthly usage data.</p> <p>Utilities must develop consistent, streamlined, “ one-stop” process for providing data to entities eligible to request access to energy data.</p> <p>All data outputs will be in standard formats. Data will be accessible in specified formats such as comma-delimited, XML, or other agreed-upon formats. Customized outputs or formats should be avoided.</p> <p>Mechanisms for handling data delivery for requests of all sizes in a secure manner should be standardized. To the extent possible, utilities will provide data through the customer data access program.</p>	
<p><b>Colorado</b></p>	<p>Public Utilities Commission of Colorado        Docket No. 10R-799E,        Decision No. R11-0922</p>	<ul style="list-style-type: none"> <li>• Types of data</li> <li>• Third party access</li> <li>• Charges for access</li> </ul> <p>8/29/2011</p>	<p>At a minimum, the utility’s tariff will provide the following:</p> <ul style="list-style-type: none"> <li>(i) A description of standard customer data and non-standard customer data (billing determinants or other collected data) and the frequency of customer data updates that will be available (annual, monthly, daily, etc.);</li> <li>(ii) The method and frequency of customer data transmittal and access available (electronic, paper, etc.) as well as the security protections or requirements for such transmittal;</li> <li>(iii) A timeframe for processing the request;</li> <li>(iv) Any rate associated with processing a request for non-standard customer data; and</li> <li>(v) Any charges associated with obtaining non-standard customer data.</li> </ul>

				<p>As part of basic utility service, a utility shall provide to a customer the customer’s standard customer data, access to the customer’s standard customer data in electronic machine-readable form, in conformity with nationally recognized open standards and best practices, in a manner that ensures adequate protections for the utility’s system security and the continued privacy of the customer data during transmission. Such access shall be provided without additional charge.</p> <p>A utility shall provide to any third-party recipient to whom the customer has authorized disclosure of the customer’s customer data, access to the customer’s standard customer data in electronic machine-readable form, in conformity with nationally recognized open standards and best practices, in a manner that ensures adequate protections for the utility’s system security and the continued privacy of the customer during transmission. Such access shall be provided without additional charge to the customer or the third-party recipient. Must provide annual notice to customers regarding data sharing.</p> <p>The utility shall make available a “consent to disclose” customer data form, prescribed and supplied by the Commission, to any customer or third-party upon request. The form shall be provided and made available in paper and electronic form for use in obtaining customer consent to disclose customer data.</p>
<p><b>New York</b></p>	<p>New York Public Service Commission          Case 10-E-0285</p>	<ul style="list-style-type: none"> <li>• Data security</li> <li>• Use of national standards</li> <li>• Third party access</li> <li>• Charges for accessing</li> </ul>	<p>8/19/2011</p>	<p>Utilities should use NIST “Guidelines for Smart Grid Cyber Security” as a reference case for best practices.</p> <p>Utilities will bear the responsibility to ensure that cost-effective protection and preparedness measures are employed to deter, detect, and respond to cyber attacks, and to mitigate and recover from their effects. Utilities should address their plans in any smart grid proposal.</p>

			data	<p>Customers are free to furnish their usage data to anyone they see fit and to establish whatever terms and conditions on the provision of such data that they deem appropriate.</p> <p>Data should be available to third parties from the utility on a timely basis when the customer authorizes it and utilities are compensated for the utility's costs of providing such access.</p> <p>Authorization for access must be affirmatively given through an opt-in process that reflects and records the customer's informed consent. The authorization must specify the purposes for which the third party is authorized to use the data, define the term during which the authorization will remain valid, and identify a means through which a customer can withdraw his/her authorization.</p> <p>Customer should have the right to access, confirm, and demand correction of their personal data.</p> <p>As data becomes more granular and detailed, more detailed and specific procedures and safeguards may be needed.</p>
<b>Pennsylvania</b>	Pennsylvania Public Utility Commission Case No. M-2010-2183412	<ul style="list-style-type: none"> <li>• Third party access</li> <li>• Types of data</li> </ul>	11/12/2010	<p>Guidelines regarding the minimum list of customer information and data points that should be included. The list included, among other things, customer account number, customer name, customer telephone number, service address, billing address, tariff rate class and schedule, rate sub-class and sub-code, meter read cycle, load profile group, monthly consumption, on-peak and off-peak consumption, monthly peak demand.</p> <p>Allowed Opt-out program.</p>
	Pennsylvania Public Utility Commission Case No. M-2010-2183412	<ul style="list-style-type: none"> <li>• Third party access</li> <li>• Data security</li> <li>• Types of data</li> </ul>	11/15/2011	<p>Continued to permit electric distribution company to use the opt-out process for customers to withhold the release of customer account and usage information from the eligible customer lists. Found the opt-out process is a reasonable and efficient means by which customers can exercise their right to</p>

				withhold confidential information.
				Removed telephone number from customer information list.
	Pennsylvania Public Utility Commission Case Nos. M-2013-2341990; M-2013-2341991; M-2013-2341993; M-2013-2341994	<ul style="list-style-type: none"> <li>Data security</li> </ul>	3/6/2014	Utilities must comply with existing legislation requiring them to develop and maintain appropriate physical security, cyber security, emergency response and business continuity plans to protect their infrastructure and ensure safe, continuous and reliable utility service.
				Companies should address security issues of smart meters at their annual stakeholder meetings.
	Pennsylvania Public Utility Commission Case No. M-2010-2183412	<ul style="list-style-type: none"> <li>Third party access</li> </ul>	10/23/2014	Utilities shall issue new opt-out solicitations every three years.
<b>Maryland</b>	Public Service Commission of Maryland, Case No. 9208, Order Nos. 83410, 83531	<ul style="list-style-type: none"> <li>Data security</li> <li>Use of national standards</li> </ul>	6/21/2010 8/13/2010	<p>The Commission initially rejected BGE’s smart grid initiative, noting the smart meter industry is currently addressing significant cyber-security and inter-operability risks.</p> <p>The Commission’s first order further noted the National Institute of Standards and Technology (“NIST”) is tasked with addressing these cyber-security concerns, but they remain a work in progress, and that NIST also is drafting standards to address issues of inter-operability between AMI vendors.</p> <p>On rehearing, the Commission approved BGE’s smart grid project.</p>
	Public Service Commission of Maryland, Case No. 9208, Order No. 85680	<ul style="list-style-type: none"> <li>Data security</li> </ul>	6/21/2013	<p>Commission noted BGE’s Smart Meter Data Privacy Policy, the purpose of which was to inform customers of the measures BGE takes to protect the confidentiality of smart meter interval data.</p> <p>The Commission approved BGE’s cyber security plan, which set forth how BGE intends to identify, monitor, and remediate risks to the confidentiality, integrity, and availability of AMI systems and data. The Commission also approved a cyber-security reporting process whereby BGE, Potomac Electric</p>

				Power Company and Delmarva Power & Light Company would report to the Commission on their cyber-security programs as well as retain and fund a cyber-security consulting firm that will be accountable to the Commission.
<b>Ohio</b>	Public Utilities Commission of Ohio Case No. 11-277-GE-UNC	<ul style="list-style-type: none"> <li>• Third party access</li> <li>• Data security</li> </ul>	5/9/2012	<p>Invited comments addressing whether Commission should consider, develop, and adopt additional rules or policies or otherwise consider smart grid related privacy or data access issues at this time, and, if so, what process and procedures should be used to address these issues.</p> <p>Found it evident from the comments and reply comments that there are numerous, complex issues that the various stakeholders believe should ultimately be addressed by the Commission in some fashion, and that coordination with the development of federal standards should be an important consideration as well.</p> <p>Directed Commission Staff to form a proposal recommending the appropriate next steps for review of consumer privacy protection and customer data access issues.</p>
	Public Utilities Commission of Ohio Case No. 12-3151-EL-COI	<ul style="list-style-type: none"> <li>• Charges for accessing data</li> <li>• Types of data</li> <li>• Data format</li> </ul>	3/26/2014	Utilities shall file amended tariffs that specify the terms, conditions, and charges associated with providing interval customer energy usage data. Tariff amendments should address or include the format, method, granularity, and frequency of customer energy usage data.
	Public Utilities Commission of Ohio, Case No. 12-2050-EL-ORD	<ul style="list-style-type: none"> <li>• Third party access</li> <li>• Data security</li> </ul>	1/15/2014	Customer specific information cannot be provided by a utility unless the customer has signed a consent form. The consent form shall be on a separate piece of paper and shall be clearly identified on its face as a release of personal information and all text appearing on the consent form shall be in at least sixteen-point type. The following statement shall appear prominently on the consent form, just prior to the signature, in type darker and larger than the type in surrounding sentences: "I realize that under the rules and regulations of the public utilities

				<p>commission of Ohio, I may refuse to allow (name of the electric utility) to release the information set forth above. By my signature, I freely give (name of the electric utility) permission to release the information designated above." The information that the electric utility seeks to release shall be specified on the form. Forms requiring a customer to circle or to check off preprinted types of information to be released may not be used.</p> <p>The Commission found that it does not believe it is the utilities' responsibility to inform customers of risks of choosing to share their information.</p>
<p><b>Texas</b></p>	<p>Public Utility Commission of Texas Project No. 31418</p>	<ul style="list-style-type: none"> <li>• Third party access</li> <li>• Types of data</li> <li>• Timeliness of data delivery</li> <li>• Data security</li> </ul>	<p>May 30, 2007</p>	<p>Commission adopted substantive rules to govern the deployment of advanced metering systems.</p> <p>Found Retail Electric Providers (“REPs”) and customers should have simultaneous, direct, password-protected, read-only access to the customer’s meter data. The Commission found that it believes that direct access to the meter data through the electric utility’s web portal as well as through a gateway inside the customer’s premise is sufficient.</p> <p>As for whether it is acceptable to have information on a day-after, day-of or instantaneous basis, the Commission concluded as long as the meters have the capability for REPs and customers to receive meter data inside the customer’s premise, hourly interval data should be provided to the web portal on a day-after basis.</p> <p>15-minute data may be offered but is not required.</p> <p>Found it is sufficient for the REP, the customer, and any authorized third party to have access to the advanced meter data via the web portal.</p> <p>An electric utility shall provide a customer, the customer’s REP, and other entities authorized by the customer read-only</p>

access to the customer's advanced meter data, including meter data used to calculate charges for service, historical load data, and any other proprietary customer information. The access shall be convenient and secure, and the data shall be made available no later than the day after it was created.

An electric utility shall use industry standards and methods for providing secure customer and REP access to the meter data.

The electric utility shall have an independent security audit of the mechanism for customer and REP access to meter data conducted within one year of initiating such access and promptly report the results to the commission.

A customer may authorize its data to be available to an entity other than its REP.

**ICC Docket No. 14-0507**

**Commonwealth Edison Company's Response to  
Illinois Commerce Commissioners' Data Requests**

**ICC 1.01-1.02**

**Date Received: October 16, 2014**

**Date Served: November 6, 2014**

**REQUEST NO. ICC 1.02:**

To the best of your ability, please provide a comprehensive list of the uniform standards or national standards recommended for adoption by States that have been developed by non-governmental third parties.

- a. Please describe their similarities and their differences when compared to the proposed Illinois Open Data Access Framework.

**RESPONSE:**

Please see the attachment labeled as ICC 1.02\_Attach 1 for a chart listing four national or uniform standards developed by the National Institute of Standards and Technology (NIST), the North American Energy Standards Board (NAESB), the Advanced Security Accelerator Project for the Smart Grid (ASAP-SG), and the Federal Smart Grid Task Force's proposed Voluntary Code of Conduct, respectively, and a comparison of these four standards to the proposed Illinois Open Data Access Framework.

**Uniform/National Standards for Collection, Management and Disclosure of Smart Grid Data:**

- A. National Institute of Standards and Technology (NIST) IR 7628 rev 1: Guidelines for Smart Grid Cyber Security: Vol 2, Privacy and the Smart Grid (September 2014) (hereinafter, the “NIST” standard);

Applicability of the Standard: “This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risk, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders ...can use the methods and supporting information presented in this report as guidance for assessing risk and identifying and applying appropriate security requirements.” (Abstract, NIST Guidelines for Smart Grid Cyber Security: Vol 2, p. iii.)

- B. North American Energy Standards Board Data Privacy Standard (REQ.22, version 2.1, August 30, 2013) (hereinafter, the “NAESB” standard);

Applicability of the Standard: “This document establishes voluntary Model Business Practices for Third Party access to Smart Meter-based Information...These Model Business Practices are intended to serve only as flexible guidelines, rather than “one-size-fits-all” requirements....these practices are not intended to apply to the Distribution Company’s disclosure, collection, use and handling of Smart Meter-based Information in connection with the Distribution Company’s or its agents’ utility services product or service fulfillment or billing or collection activities. Instead they are intended solely to apply to other disclosures of Smart Meter-based Information from the Distribution Company to a Third Party, as well as the collection, use and retention of Smart Meter-based Information by such Third Party and the disclosure of Smart Meter-based Information from one Third Party to another Third Party.” (Executive Summary, p. 7.)

- C. Security Profile for Third Party Data Access, The Advanced Security Acceleration Project for the Smart Grid (version 1.0, dated May 18, 2011) (hereinafter, the “ASAP-SG standard”);

Applicability of the Standard: “This document delineates the security requirements for individuals, utilities, and vendors participating in a three-way relationship that involves the privacy and handling of sensitive data. Specifically this document is aimed at the smart grid environment, and is intended to address the concerns of electric utility customers who want to allow value added service providers to access electric usage data that is in the custody of the customer’s utility. Other three-way data sharing scenarios may also be addressed using this profile, as the roles of the three parties have been abstracted in such a way as to support mapping to

different environments.” (Executive Summary, p. iii.) This document is primarily a technical security profile, and it presumes that the data subject (customer) has consented to the sharing of data with a third party. For this reason, it is only cited below in that context.

D. Data Privacy and the Smart Grid: A Voluntary Code of Conduct, developed by the U.S. Department of Energy’s Office of Electricity Delivery and Energy Reliability and the Federal Smart Grid Task Force (Aug. 12, 2014 Draft) (hereinafter, the “DOE VCC”).

Applicability: “The [Voluntary Code of Conduct “VCC”]’s recommendations are intended to apply as high level principles of conduct for both utilities and third parties. The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, it is envisioned that the VCC could be most beneficial to either entities that are not subject to regulation by applicable regulatory authorities, or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines. The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could potentially adopt the principles of the VCC with some limited exception, such as when laws, regulatory guidance, governing documents, and/or prevailing state/local business practices indicate a different approach.” (Mission Statement, p.1).

The following table identifies relevant provisions in the above-referenced national standards and notes the similarities and differences between those and the proposed Illinois Open Data Access Framework:

<u>Proposed Illinois Open Data Access Framework</u>	<u>National Standards</u>
<b>1. Ownership</b>	
<p>Customer is principal owner of retail electric consumption data. The customer has the ability to authorize third parties to access individual customer data, and the customer can revoke that access at the customer’s discretion.</p> <p>The utility serves as the guardian of retail electric consumption data, and must allow access to third parties where the customer has authorized it.</p>	<p>(a) NIST</p> <p>The authors of the NIST standard note that data ownership is subject of “much discussion” but they do not assert a position on it; instead focusing on privacy considerations and the proper <i>safeguarding</i> of personal information. The NIST standard suggests that ownership be viewed “...as a question of who should have what rights to the data (e.g., right to control, right to exclude, etc.) These rights may be divided or shared among multiple entities. Alternatively, entities that have the ability to control or manage the data may have some responsibilities regarding the</p>

	<p>data, regardless of ‘ownership.’” §5.3.2.2 Smart Grid Data Ownership p. 15.</p> <p>(b) NAESB, ASAP-SG and the DOE VCC do not expressly address ownership.</p> <p><u>Similarities/Differences</u></p> <p>The concept of customer ownership of energy usage data as set forth in the IODA Framework is notably different from the four standards noted above, none of which take an express position on ownership. With respect to the utility as “guardian” and a requirement of disclosure to third parties upon customer’s authorization, see “Third Party Access” below.</p>
<p><b>2. Type of Data</b></p>	
<ul style="list-style-type: none"> <li>• <b>Interval.</b> Customers should have access to their retail electric consumption data in as short intervals as possible, with 15-minute intervals recommended, but never in intervals greater than 1-hour. This includes power (kW) and energy (kWh) at the designated intervals.</li> <li>• <b>Consumption.</b> Customers should have access to the monthly aggregate retail electric consumption data used for billing purposes.</li> <li>• <b>Power data.</b> Any data relating to demand, power quality, availability, voltage, frequency, current, power factor, or other information generated by a meter should be made available to both the customer and the utility.</li> <li>• <b>Pricing.</b> Customers should have access to any and all price and rate data at the time for which they are being charged that</li> </ul>	<p>(a) NIST        “Any organization possessing energy data about consumers should provide a process to allow consumers access to the corresponding energy data for their utilities account.” §5.12 Smart Grid Privacy Summary and Recommendations (Subsec. 6: Individual Access) p. 55.</p> <p>(b) NAESB        The NAESB standard directs that both utilities and third parties should develop and communicate to customers processes for such customers to have access to smart meter data for such customer. (REQ.22.3.6. Individual Access, p. 20.)</p> <p>(c) DOE VCC        The DOE VCC identifies “Customer Data Access and Participation” as one of five core concepts, stating “...customers should have access to their own [c]ustomer [d]ata and should have the ability to participate in its maintenance.” (§3, p. 9.)</p>

<p>rate. For price and rate data that is known in advance (day-ahead, TOU), price and rate data should be available to a customer for the duration of the price and rate data availability preceding the effective time.</p>	<p><u>Similarities/Differences:</u>          While the IODA Framework and the above-referenced standards share the general concept of providing customers with access to their usage data, none of the above referenced standards require that data be gathered or made available at specific interval levels, nor do they address the topics identified under the IODA Framework’s subheadings “Power data” or “Pricing”.</p>
<p><b>3. Third Party Access</b></p>	
<ul style="list-style-type: none"> <li>• <b>Definition:</b> Third parties are defined as any entity not including the customer or utility that is seeking access to retail electric consumption data.</li> </ul>	<ul style="list-style-type: none"> <li>(a) NIST            The NIST standard defines a “third party” as “[a]n entity – other than the electric utility or other electricity provider for a given premise, the applicable regulatory authority, an independent system operator (ISO) or another regional entity – that performs or provides products using CEUD (Customer/Consumer Energy Usage Data). This definition does not include Contracted Agents of an electric utility or electricity provider.” (Rev. 1, Appendix D)</li> <li>(b) NAESB            The NAESB definition of a “Third Party” is an entity “that is permitted to receive Smart Meter-based Information in accordance with applicable law, regulation...” other than a regulated utility, regulatory authority, or independent system operator. (REQ.22.2.2t).</li> <li>(c) ASAP-SG            “... we assume a third party to be any entity that requests access to data in the custody of someone besides the [data] subject.” (§1, p. 3.)</li> <li>(d) DOE VCC            The DOE VCC defines “Third Party” as an entity requesting access to Customer Data for a Secondary Purpose (materially different from the purpose the customer reasonably expects or purpose initiated by customer) (Key Definitions, p. 3).</li> </ul>

	<p><u>Similarities/Differences:</u>          The IODA Framework definition is most similar to that of the ASAP-SG in that it is a broad, encompassing definition of “third party.” The NAESB definition is fairly different in that it limits the definition to parties who <u>have been authorized</u> by the customer to receive the data. The DOE VCC definition is different in that it is tied to the <u>purpose</u> for which the data is sought.</p>
<ul style="list-style-type: none"> <li>• <b>Customer Authorization.</b> Customers wishing to provide access to their customer-specific retail electricity consumption data to any third party must affirmatively authorize the third party to gain access.</li> </ul>	<p>(a) NIST          The authors of the NIST standard note that “the bulk of the work on these recommended privacy practices occurred after the California Public Utilities Commission (CPUC) issued its smart grid data access rules, the North American Energy Standards Board (NAESB) released its guidelines (REQ22) on this subject, and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Group released their recommendations. Those efforts applied to utilities and Third Parties obtaining access to data from those utilities. The purpose of this group’s effort was to apply the same type of recommended protections to Third Parties that gain access to CEUD directly from customers or customer-owned devices, bypassing the utility and the smart meter.” (Appendix D; §D-1). As such, the NIST standard does not apply to the initial authorization for a third party, but it does assert that in the context of a disclosure by an authorized third party to another third party, that customer authorization is again required. §5.7.3, p. 38.</p> <p>(b) NAESB          The NAESB standard directs that a utility should not disclose Smart meter-based Information to a third party without obtaining and/or verifying authorization from the customer, as permitted or required by law / regulation. (REQ.22.3.3.1.1)</p>

	<p>(c) ASAP-SG        The ASAP-SG standard by its own terms only applies to situations where a data subject (such as a residential utility customer) grants permission to share its data with a third party so that the third party can perform a desired service for the data subject. (§1.1, p. 4). As such, it does not contemplate the threshold question of whether consent is required, although in the description of the role of the data custodian (typically the utility), it notes “A Data Custodian manages resource information on behalf of a Data Subject and will share this information with Third Parties only in accordance with the wishes of the Data Subject.” (§2.1.2, p. 8)</p> <p>(d) DOE VCC        Recommends customer’s consent for disclosure of Customer Data for “Secondary Purposes” (materially different from the purpose the customer reasonably expects or purpose initiated by customer) be specifically and affirmatively expressed before data is shared; specifically excludes aggregated data from consent requirement. §2, pp. 6-7.)</p> <p><u>Similarities/Differences:</u>        The principle of customer consent prior to disclosure of usage data to third parties appears to be fairly universal. Differences among the cited standards and the IODA Framework stem largely from the existence of, (in the case of the DOE VCC for example) or absence of, (in the case of the IODA Framework) express exceptions for (i) use of the data for primary purposes, or (ii) use of aggregated or de-identified data.</p>
<ul style="list-style-type: none"> <li>• There should be no distinction drawn between the type of usage data given to third parties with customer authorization now and</li> </ul>	<p><u>Similarities/Differences:</u>        None of the national standards identified above address the distinction of AMI- vs. non-AMI data.</p>

<p>what usage data will be available following deployment of AMI. Currently authorized third parties should receive interval usage data as it becomes available to customers who have already authorized the same third party access to their usage data.</p>	
<ul style="list-style-type: none"> <li>The authorization process must be simple, practical, and rapid for the customer.</li> </ul>	<p>(a) NIST        The NIST Standard recommends that consumer notifications (including those related to any choices available to the consumer about information being collected and any explicit consents) be “clearly worded.” (§5.12, subsection 3, p. 55).</p> <p>(b) NAESB        The NAESB Standard states that any “Authorization terms and conditions regarding disclosure of Smart Meter-based Information to Third Parties should be reasonably clear, concise, understandable and accessible, subject to [applicable laws and regulations].” (REQ. 22.3.2.1.2).</p> <p>(c) ASAP-SG        The premise of the security requirements set forth in the ASAP-SG is that the data subject (customer) has already granted permission for the data custodian (such as a utility) to share the usage data about the data subject. (§1.1, p. 4). As such, it is silent on this point.</p> <p>(d) DOE Voluntary Code of Conduct        Consent process should be “convenient, accessible, and easily understood...” (§2, p. 4).</p> <p><u>Similarities/Differences:</u>        The IODA Framework requires that the consent authorization process for the customer be “simple, practical and rapid.” The standards noted above have a similar emphasis, to the extent that “simplicity” can be</p>

	<p>equated with clarity – the latter being an emphasis in the three relevant standards. The national standards, however, also have a slightly different emphasis, on accessibility. One difference between the IODA Framework as compared to the national standards is the framework’s reference to the process of authorization being “rapid.” None of the national standards have any reference to speed in this regard.</p>
<ul style="list-style-type: none"> <li>○ Authorization should be available to customers through the same method as the provision of data where practical (e.g., directly from the meter, through the internet, through mobile devices) using the most convenient method for the customer. Although a customer’s non- electronic signature should not be not required to indicate authorization, such a signature is acceptable if the customer and third party determine it is more convenient/appropriate than alternative verbal or electronic methods. A non-electronic signature may be preferred in the case of parties who must attest to the utility having obtained customer authorization on behalf of large groups of customers.</li> </ul>	<p><u>Similarities/Differences:</u>          While all of the national standards discussed above contemplate some form of consent by the customer to third parties (as discussed above), none specifically require that the authorization be made available through the same method as the provision of data, nor do they address the method of signature for consent (or whether a signature is required or desirable).</p>
<ul style="list-style-type: none"> <li>○ For Retail Electric Suppliers (RES), the authorization should last until the customer leaves the service of that RES, unless a customer affirmatively de-authorizes access to data. No distinction should be drawn between those customers who change supply service via municipal aggregation and those</li> </ul>	<p><u>Similarities/Differences:</u>          None of the national standards listed above have specific requirements with respect to retail electric suppliers, nor do they address the distinction between changes due to municipal aggregation vs. individual preference. The national standards do, however, address termination of previously granted consents to share data with third parties (see below.)</p>

<p>who switch due to their individual preference (“organic” customers).</p>	
<p>○ Data should be maintained for the entire history of an account.</p>	<p>(a) NIST        The NIST standard expressly recommends limiting information retention. “Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfill the purposes that have been communicated to the energy consumers. After the appropriate retention period, data should be aggregated or destroyed.” (§512, Subsec. 5 “Use and Retention” p. 55).</p> <p>(b) NAESB        The NAESB standard appears to be silent on the issue of duration of retention by the utility, but it does limit the duration of retention by an authorized third party to “as long as is necessary to fulfill the Authorized Purposes for which it was collected.” Subject to any retention period specified by law or regulation. REQ.22.3.5.</p> <p>(c) ASAP-SG        The ASAP-SG standard appears to be silent on this issue.</p> <p>(d) DOE VCC        The DOE VCC states “Service Providers should retain Customer Data only as long as needed to fulfill the purpose it was collected for, unless they are under a legal obligation to do otherwise.” (§2, Subsec. 1 “Records Retention and Disposal,” p. 7)</p> <p><u>Similarities/Differences:</u>        None of the national standards set forth requirements regarding maintaining the “entire history” of an account, in fact several contradict this concept.</p>
<p>○ For all other third parties, the authorization</p>	<p>(a) NIST</p>

<p>should last for a term of 24 months, unless a customer affirmatively de-authorizes access to data. Data should be maintained for the entire period of authorization.</p>	<p>NIST requires the customer to be informed of how they can revoke their authorization for a third party to have and use their energy usage data (§5.7.3, pp. 37-38).</p> <p>(b) NAESB        If customer authorization for disclosure to third parties was granted for a specified or an indeterminate period, the NAESB standard dictates that the utility should terminate such third party’s access when (i) customer recinds the authorization, (ii) the authorization was for a specified period and the period expires, (iii) when the customer terminates service associated with a particular premises, or (iv) as required by law or regulation. (REQ 22.3.3.1.5)</p> <p>(c) ASAP-SG        The ASAP-SG standard provides examples of customer-initiated termination or modification of permissions previously granted to third parties. (§2.4.3 and §2.4.4, pp. 20-23).</p> <p>(d) DOE VCC        Customer authorization for disclosure to third parties expires when (i) customer recinds it, (ii) authorization expires [presumably by its own terms], or (iii) the customer terminates service. (§2(h), p. 6).</p> <p><u>Similarities/Differences:</u>        All four standards contemplate the customer having the ability to revoke (and in some cases modify) a previously granted third party authorization but none contain support for the 24-month standard in the IODA Framework.</p>
<p>o The de-authorization process must similarly be simple, practical, and rapid for the customer.</p>	<p>(a) NIST        No specifics on the de-authorization process.</p> <p>(b) NAESB        The NAESB standard requires the method for the withdrawal of</p>

	<p>customer authorization for disclosure to a third party to be “reasonable.” (REQ.22.3.3.1.4)</p> <p>(c) ASAP-SG        The ASAP-SG standard provides technical guidance on how the de-authorization process should work but does not address the nature of the process for the customer.</p> <p>(d) DOE VCC        The DOE VCC requires that the customer have notice of how the customer can revoke previously granted third party access to their data but does not direct the nature of such process for revocation. (§1(f), p. 5.</p> <p><u>Similarities/Differences:</u>        All four standards contemplate the customer having the ability to revoke (and in some cases modify) a previously granted third party authorization but only the NAESB standard addresses the nature of the process for revocation, requiring it to be “reasonable.” In contrast to the IODA Framework, none of the national standards address the speed of the process.</p>
<ul style="list-style-type: none"> <li>○ Once customer authorization has been given to a third party, the same standards that apply to the access of third parties that have obtained customer authorization should also apply to RES access to such data.</li> </ul>	<p><u>Similarities/Differences:</u>        We find no support in any of the national standards for the expansion of a customer’s authorization to one third party to other third parties.</p>
<ul style="list-style-type: none"> <li>○ There is no distinction between data that is used for billing purposes with data that is used for non-billing purposes. The <i>purpose</i> of the data (billing vs. non-billing purposes) should be distinct from the <i>quality</i> of the data (preliminary vs. bill-quality data). Once a third party obtains a customer’s authorization</li> </ul>	<p>(a) NIST        The NIST standard, citing the Fair Information Practice Principles (FIPPS), asserts that “a Third Party should not be collecting more than what is required to fulfill the agreed upon service, and a separate customer authorization should be obtained before CEUD is used in a materially different manner.” §5.7.3 (Data Disclosure and Minimization), p. 38.</p>

to access that customer's interval data, that third party effectively stands in the shoes of the customer and as such, no additional authorization is needed.

(b) NAESB

The NAESB standard restricts third party collection of Smart Meter-based Information to "only that information necessary to fulfill the purpose (e.g. to provide a service or product, etc.) as set forth in the Retail Customer's Authorization." (REQ.22.3.4.1.1)

(c) ASAP-SG

The security protocols in ASAP-SG are premised on the assumption that "the Data Subject wants certain pieces of their information to be shared with parties they select. Conversely, it is assumed that the Data Subject does not necessarily want all of their information shared." (§2.3, p. 13).

(d) DOE VCC

The DOE VCC contemplates customers being able to control and authorize third party access to the customer's data, including the ability to authorize "different types of disclosures of his or her Customer Data among multiple third parties" and specifically requiring customer authorization for any disclosure to a third party for a Secondary Purpose (a purpose that is materially different from the Primary Purpose of the disclosure and is not reasonably expected by the customer relative to the transactions or ongoing services provided to the customer.) §2(c) and (e), and Key Definitions.

Similarities/Differences:

We find no support in any of the national standards for the expansion of a customer's authorization to one third party to other third parties. The assertions in the IODA Framework that (i) there is no distinction with respect to the purpose of the data and that (ii) once authorization has been given to a third party that such party "stands in the shoes of the customer" are in direct contrast with the national standards. The

	<p>national standards emphasize the purpose for which data is being disclosed as a key element of the third party authorization, and restrict third parties' access to customer data to the express purposes authorized by the customer.</p>
<ul style="list-style-type: none"> <li>▪ For customers who have not yet authorized a third party access to their usage data, authorization must be given that explicitly references “interval usage data” and makes the customer aware that data will be used by the third party to deliver the services being provided but also to develop new services which could be offered to the customer.</li> </ul>	<ul style="list-style-type: none"> <li>(a) NIST        The NIST standard recommends that “[a]ny organization collecting energy data from or about consumers should establish a process to notify [customers]...in a clearly worded description of the data being collected, why it is necessary to collect the data, the intended use, retention, and sharing of the data.” §512, subsec. 2, p. 54.</li> <li>(b) NAESB        The NAESB standard requires “reasonably conspicuous and clear notice to Retail Customers that Smart Meter-based Information will not be disclosed to Third Parties, unless such disclosure is Authorized by the Retail Customer. REQ.22.3.2.1.1</li> <li>(c) ASAP-SG        As noted above, the ASAP-SG standard presumes that notice has already been given. It does not specific the contents of the notice.</li> <li>(d) DOE VCC        The DOE VCC adopts as a core concept that notice should be given to customers regarding the specific types of information being collected and how it will be used. §1(a)-(j), pp. 4-5.</li> </ul> <p><u>Similarities/Differences:</u>        All of the national standards are similar to the IODA Framework in the general concept that customers should receive a clear disclosure of the nature of data being collected and the purposes for which it may be used and shared. The IODA Framework differs from the national standards in the requirement of specifying “interval usage data” in the</p>

	<p>notice, and in the proposed automatic permission for third parties to use data not only for the services being provided but also “to develop new services.” The national standards typically require that consent for one purpose does not imply consent for any other purpose.</p>
<ul style="list-style-type: none"> <li>▪ For customers participating in a municipal aggregation, Retail Electric Suppliers must disclose that access to interval usage data may be used to develop new services beyond what are offered in the aggregation. Authorization for these purposes shall be separately given, as per the Final Order in ICC Docket No. 13-0506, and must be separate from authorization to participate in the aggregation and/or select a new supply service.</li> </ul>	<p><u>Similarities/Differences:</u>          The national standards do not address this topic.</p>
<p>• <b>Scope of Access</b></p>	
<ul style="list-style-type: none"> <li>○ Third parties should be provided access to any and all data (see “Type of Data” and “Forms”) when affirmatively authorized by a customer.</li> </ul>	<p><u>Similarities/Differences:</u>          All four national standards acknowledge a right of access to the data for the customer (see discussion under “Type of Data” above) and the concept of customer authorization for disclosures to third parties (see “Customer Authorization” above).</p>
<ul style="list-style-type: none"> <li>○ Where a third party seeks access to customer usage data without customer authorization, the scope of access can be no more limited than allowed by the 15/15 Rule as adopted by the Commission in ICC Docket No. 13-0506. In summary, the 15/15 Rule permits utilities to provide to third parties 12 months of anonymized customer usage data of at least 15 customers within a customer class</li> </ul>	<p>(a) NIST          The NIST standard does not adopt a standard for aggregation, but does recognize an exception to the customer consent requirement for disclosure of aggregate data when the customer “... has already authorized a particular service or product, and a Third Party or Third Party’s Contracted Agent needs to disclose aggregated or de-identified information in order to produce that service or product.... so long as that information cannot be tracked back to an individual or used to identify a customer.” Appendix D §3.3,</p>

<p>organized by groups of customers within the same ZIP+4 such that no one customer's usage data comprises more than 15% of the customer group.</p>	<p>pp. 71-72.</p> <p>(b) NAESB        The NAESB standard permits utilities to “disclose aggregated Smart Meter-based Information to Third Parties without Retail Customer Authorization, if that information does not identify and cannot be reasonably traced back to individual Retail Customers, and as otherwise permitted [by law or regulation].” REQ 22.3.7.1.2.</p> <p>(c) ASAP-SG        This standard does not discuss aggregated data.</p> <p>(d) DOE Voluntary Code of Conduct        The DOE VCC expressly permits disclosure of “Aggregated or Anonymized Data” as long as the method of aggregation or anonymization “strongly limits the likelihood of reidentification of individual customers or their Customer Data...” §2, subsec. 4, p. 7</p> <p><u>Similarities/Differences:</u>        In contrast to the IODA Framework, the national standards characterize the ability to share aggregate, de-identified data with third parties without consent as an <u>exception</u> to the general rule that customer consent is required before third parties can receive access to customer data. The IODA Framework's characterization of a restriction on the scope of access by third parties implies a presumed right of access by third parties. The national standards presume the opposite: that no access by third parties is permissible without express consent.</p>
<ul style="list-style-type: none"> <li>• <b>Conditions on Access.</b> The utility may institute a process for approval of third parties who wish to obtain access to customer-specific data if such requirements are related to data security, and the ability to receive the transmission of data in an</li> </ul>	<p><u>Similarities/Differences:</u>        None of the national standards create such an exception to the rule requiring consent for disclosure to third parties.</p>

efficient manner	
<b>4. Format</b>	
<ul style="list-style-type: none"> <li>• <b>Machine-readable.</b> Customers or affirmatively-authorized third parties should be provided access to their raw retail electricity consumption data in an industry-standard or web-standard machine-readable format (e.g. XML).</li> <li>• <b>Summary.</b> In order to provide education to customers about consumption behavior and enable opportunities for behavior change, customers should be able to access their retail electricity consumption data in a summary format that is intended to influence specific or general customer behavior (e.g. display of consumption during peak-time events).</li> <li>• <b>Monthly Billing.</b> Customers should be able to see all the components of their retail electricity consumption data used for billing on their monthly billing statement. This includes consumption aggregated by rate type for customers on dynamic or time-of-use rate plans.</li> </ul>	<p><u>Similarities/Differences:</u>          None of the national standards dictate the format in which electric usage data must be delivered.</p>

<b>5. Methods of Delivery</b>	
<ul style="list-style-type: none"><li>• <b>Directly from the meter.</b> Usage data should be provided directly from a meter. Any and all data that is generated and transmitted by the meter should be in machine-readable formats.</li><li>• <b>Directly through the internet.</b> Usage data should be provided directly through the internet from the utility in machine-readable formats.</li><li>• <b>Through a Web Portal.</b> Billing and usage data should be provided in downloadable, comprehensive, and summary forms through web portals operated by utilities or other third-party systems which meet utility security requirements, including utility vendors.</li><li>• <b>Through mobile applications.</b> Billing and usage data should be provided. Customers should be able to access timely downloadable, comprehensive, and summary data through mobile applications operated by utilities or other third party systems which meet utility security requirements, including utility vendors.</li><li>• <b>Bulk Transfers.</b> For the purposes of efficiency, the utility may maintain a separate process for providing bulk or aggregate customer-specific retail electric consumption data to third parties.</li></ul>	<p><u>Similarities/Differences:</u> None of the national standards address or require specific methods of delivery.</p>

<b>6. Timeliness</b>	
<p>Once recorded, data should be delivered to the customer in a timely fashion as described below.</p> <ul style="list-style-type: none"> <li>• <b>Real-time.</b> The utility and third parties shall deliver consumption data to customers in real-time to the extent practical.</li> <li>• <b>1 Hour through Internet/Alternate Communications Network.</b> To the extent practical, customers and affirmatively-approved third parties should have access to their retail electric consumption data within one hour from the conclusion of an interval period, when accessed directly from the internet or alternate communications network in a machine readable format.</li> <li>• <b>1 Minute directly from the meter.</b> To the extent practical, customers or affirmatively-approved third parties should have access to their retail electric consumption data within 1 minute when accessed directly from the meter.</li> </ul>	<p><u>Similarities/Differences:</u>          None of the national standards address or require specific timeframes for delivery.</p>
<b>7. Billing-Quality Data</b>	
<ul style="list-style-type: none"> <li>• Where there is a need for utility meter data management systems and billing systems to verify usage data for the purposes of customer billing, such processes should not limit customer access to data available from a meter as soon as it is available. Customers and affirmatively-approved third parties should be able to gain timely access to both</li> </ul>	<p><u>Similarities/Differences:</u>          None of the national standards address or require specific timeframes for access or requirements related to “preliminary” vs. “billing-quality” data.</p>

<p>preliminary data and billing-quality data.</p> <ul style="list-style-type: none"> <li>• <b>Preliminary Data.</b> Data from the meter that has not yet gone through billing system processes for quality assurance. This data may be labeled as “preliminary data.” This data must [be] replaced or separately distinguished from billing-quality data once billing-quality data is available</li> <li>• <b>Billing-quality data.</b> Data that is sufficient for billing purposes.</li> </ul>	
<p><b>8. Data Security</b></p>	
<ul style="list-style-type: none"> <li>• <b>Industry-standard protocols.</b> Data transmission to customers or third parties must be done using industry-standard secure communications and encryption protocols for wireless or network communications (e.g. HTTPS).</li> <li>• <b>Data storage.</b> Customer-specific data stored by the utility or third parties should be secured against unauthorized access using industry-standard cyber security protections. The same data security protections and restrictions on personally identifiable information that apply to the utility shall apply to any third party approved to receive customer-specific data.</li> </ul>	<ul style="list-style-type: none"> <li>(a) NIST The NIST standard does not specifically require a particular protocol, but rather contains numerous references and discussions of the benefits and vulnerabilities of various types of encryption and other security technologies.</li> <li>(b) NAESB The NAESB standard states that utilities should develop and incorporate “information privacy protections” for stored data but it does not specify protocols. REQ 22.3.8.1.1.</li> <li>(c) ASAP-SG This standard is specific to the sharing of data with third parties, and references the security controls described in the Smart Grid Security Profile Blueprint (ASAP-SG, 2009).</li> <li>(d) DOE VCC DOE VCC recommends customer data be protected via a cybersecurity risk management program (and gives some high-level guidelines for such a program) – no specific encryption requirement. §4, p. 10.</li> </ul> <p><u>Similarities/Differences:</u>    All of the national standards contemplate the use of security controls</p>

	<p>by both utilities and third parties who receive customer data, and further contemplate the reality that technology is constantly changing. This appears to be a similarity with the IODA Framework, which, by its use of the term “industry-standard” appears to contemplate that the appropriate security controls may change over time. The differences are primarily with the IODA Framework’s identification of encryption specifically, as a required protocol.</p>
<p><b>9. Following National Standards</b></p>	
<ul style="list-style-type: none"> <li>For the format and methods of provisioning customers with their retail electric consumption data from utility systems, the utility shall follow standards and protocols developed through national, multistakeholder processes. However, a utility shall not be constrained by being the first utility to implement standards developed through such processes.</li> </ul>	<p><u>Similarities/Differences:</u>          None of the four national standards reviewed address the format or method of providing customers with electric data.</p>
<p><b>10. Customer Charges</b></p>	
<ul style="list-style-type: none"> <li>Customers and affirmatively-authorized third parties should incur no additional charge for the provision of their retail electric consumption data in a timely, accessible manner to themselves or their third party designee in the manners described herein.</li> </ul>	<ul style="list-style-type: none"> <li>(a) NIST              This standard does not address the issue of additional charges for customer authorization of third party data access.</li> <li>(b) NAESB              This standard does not address the issue of additional charges for customer authorization of third party data access.</li> <li>(c) ASAP-SG              This standard does not address the issue of additional charges for customer authorization of third party data access.</li> <li>(d) DOE VCC              DOE Voluntary Code of Conduct suggests that service providers be permitted to charge a fee for non-standard requests (custom interval, custom format) for individual data or aggregate data. (§2 (i), p. 6).</li> </ul>

Similarities/Differences:

While all four national standards acknowledge a right of access to the data for the customer (see discussion under “Type of Data” above), three of the four standards reviewed do not address the issue of charges for access. The DOE VCC is directly dissimilar to the proposed IODA Framework in that it does contemplate the utility charging for certain non-standard access requests.