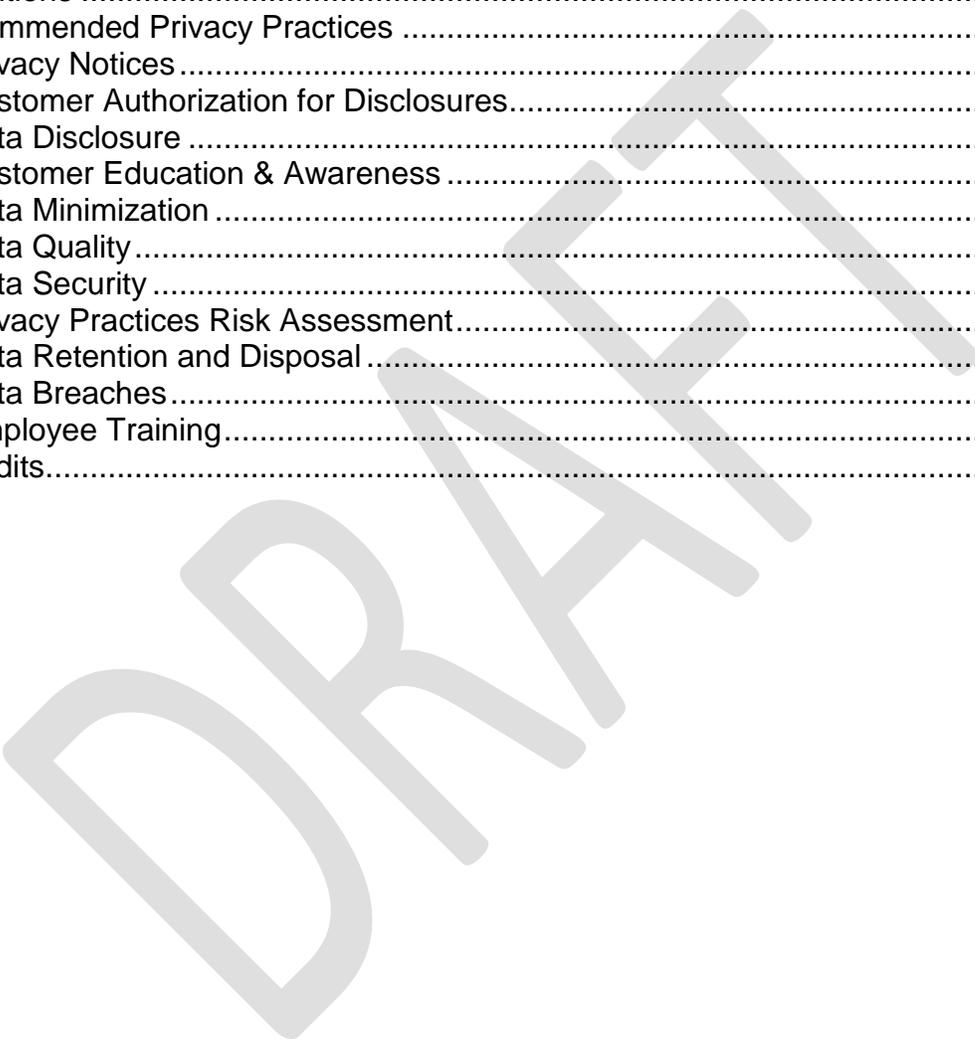


**Recommended Privacy Practices for Customer/Consumer Smart
Grid Energy Usage Data Obtained Directly by Third Parties**

SGIP Cyber Security Working Group, Privacy Subgroup
August 13, 2012

Preamble..... 1
Definitions 1
Recommended Privacy Practices 2
 Privacy Notices..... 2
 Customer Authorization for Disclosures..... 3
 Data Disclosure 4
 Customer Education & Awareness 5
 Data Minimization 5
 Data Quality 5
 Data Security 5
 Privacy Practices Risk Assessment..... 5
 Data Retention and Disposal 6
 Data Breaches..... 6
 Employee Training..... 7
 Audits..... 7



1 Preamble

2 The Customer/Consumer Energy Usage Data Privacy Protection team has developed the
3 following recommended privacy practices for application to energy customers and the third
4 parties with whom they share Customer/Consumer Energy Usage Data (CEUD). While the
5 work of this group began early in 2011, the bulk of the work on these recommended privacy
6 practices occurred after the California Public Utilities Commission (CPUC) issued its smart grid
7 data access rules, the North American Energy Standards Board (NAESB) released its
8 guidelines (REQ 22) on this subject, and the Advanced Security Acceleration Project for the
9 Smart Grid (ASAP-SG) group released their recommendations. Those efforts applied to utilities
10 and third parties obtaining access to data from those utilities. The purpose of this group's effort
11 was to apply the same type of recommended protections to third parties that gain access to
12 CEUD directly from customers or customer-owned devices, bypassing the utility and the smart
13 meter. The goal of the group was to expand upon the good work already done.

14
15 These are recommended privacy practices that should be implemented in a comprehensive
16 manner and not considered individually. If individual recommendations are taken out of context,
17 they may not stand on their own. While there may exist uncertainty over the extent to which any
18 one government agency has regulatory oversight of third parties using CEUD, many agree that
19 energy usage data (that will soon become more prevalent as the electric grid gains increased
20 intelligence) can potentially be sensitive, privacy-impacting, data in need of protection. This is
21 particularly true when CEUD is combined with other data, such as an account number or AMI IP
22 address, that then makes it identifiable to one premise or customer. These recommended
23 privacy practices seek to provide suggestions as to how CEUD, and the data combined with it
24 as just described, is best protected in order to protect personal privacy.

25 Definitions

26
27 **Customer:** Any entity that takes electric service for its own consumption.

28
29 **Third Party:** An entity — other than the electric utility or other electricity provider for a given
30 premise, the applicable regulatory authority, an independent system operator (ISO) or
31 another regional entity— that performs services or provides products using CEUD. This
32 definition does not include contracted agents of an electric utility or electricity provider.

33
34 **Contracted Agent:** An entity under contract with the Third Party to perform services or provide
35 products using CEUD. In some industries, Contracted Agents are referred to as
36 Business Partners or Business Associates.

37
38 **Customer/Consumer¹ Energy Usage Data (CEUD):** Energy usage information and data
39 identifiable to a premise or an individual Customer obtained without the involvement of
40 the utility.

41

¹ There may be a legal issue in terms of who has access to this data. There may be situations in which the Customer and the consumer are not the same and that one might want to restrict access to the CEUD. These recommended practices are not designed to determine legal issues.

42 **Privacy Use Case:** A method of looking at data flows that will help Third Parties to rigorously
43 track data flows and the privacy implications of collecting and using data, and will help
44 the organization to address and mitigate the associated privacy risks within common
45 technical design and business practices. Use cases can help Smart Grid architects and
46 engineers build privacy protections into the Smart Grid.
47

48 **Recommended Privacy Practices**

49 **Privacy Notices**

50 **When a Privacy Notice Is Issued**

- 51 • Prior to sharing CEUD, Third Parties should provide clear and conspicuous² notice to
52 Customers regarding data treatment and that CEUD will not be disclosed to other Third
53 Parties unless authorized by the Customer (with all exceptions listed).
- 54 • Notice to the Customer of all intended disclosures should be re-issued at least annually.
- 55 • Re-issue should occur when significant changes are made to operational or
56 organizational structure of the company that may impact privacy or security of the data.
57 A few examples may include:
 - 58 1) a merger or acquisition of the company
 - 59 2) when declaring bankruptcy³
 - 60 3) when services which were not previously outsourced are.
- 61 • Re-issue should also occur when major changes occur within the organization that may
62 reasonably impact the company's data privacy practices relating to disclosing CEUD to
63 Third Parties or Third Party's Contracted Agents, such as when new applicable laws
64 and/or regulations become effective.
- 65 • Customer notice should come from the Third Party with which the Customer has a
66 business relationship. Any entity that is not directly involved with the transaction being
67 considered need not send a separate notice.⁴

68 **What Should Go Into a Privacy Policy Notice**

- 69 • Privacy policy notices should include information about how the Third Party will access,
70 collect, use, store, disclose, retain, dispose of, and safeguard CEUD.

² For one example of what is considered "clear and conspicuous," see the Federal Trade Commission's document entitled "Dot Com Disclosures: Information About Online Advertising," page 5, at <http://business.ftc.gov/sites/default/files/pdf/bus41-dot-com-disclosures-information-about-online-advertising.pdf>.

³ <http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=2180>, and <http://epic.org/privacy/airtravel/clear/>.

⁴ This is to clarify who among the common actors (Third Parties and Contracted Agents) needs to send a privacy policy notice to Customers.

- 71 • Information about data access that will or may be given to a Third Party's Contracted
72 Agent should be provided in the initial notice to the Customer. The notice may be listed
73 by service (e.g., data formatting, billing) instead of contractor's company name.
- 74 • Separate notice is not necessary for the sharing of CEUD with a Third Party's
75 Contracted Agent, unless the purpose is materially different than has been previously
76 authorized.
- 77 • Third Parties should provide Customers with a process for addressing their CEUD
78 privacy complaints. This process, which may include existing procedures established or
79 approved by the applicable regulatory authority or other legal requirements, should be
80 discussed in the notices to the Customer.
- 81 • A Customer's right to revoke authorization should be reiterated in the periodic privacy
82 notice sent to Customers.
- 83 • Breach notification processes should be communicated to Customers by the Third Party
84 as part of the periodic privacy notice.⁵
- 85 • All information privacy policies regarding disclosure to other Third Parties or the Third
86 Party's Contracted Agents should be clear, concise (notice should be no longer than is
87 necessary to convey the requisite information), understandable, and easily accessible.

88 **Customer Authorization for Disclosures**

- 89 • Data should not be disclosed to other Third Parties unless there is an authorization to do
90 so by the Customer. This authorization should notify the Customer of the identity of the
91 other Third Parties.
- 92 • When the Third Party obtains the Customer's authorization, it should identify any choices
93 available to the Customer regarding CEUD disclosure as part of the authorization
94 process (e.g., the ability to opt-out of disclosure).

95 **Disclosure to Contracted Agents**

- 96 • Third Parties and Third Party's Contracted Agents do not need further Customer
97 authorization in order to provide services or products, or to fulfill other obligations to
98 Customers, that have already been authorized by the Customer.⁶
- 99 • Before releasing CEUD to a Third Party's Contracted Agent, Third Parties should receive
100 confirmation that the Third Party's Contracted Agent has security and privacy safeguards
101 in place at least equal to those implemented by the Third Party.

102 **Customer Access to Their Data**

- 103 • A Third Party should develop and communicate processes for a Customer to have
104 access to their CEUD and to be able to request that the CEUD be corrected where
105 inaccuracies exist. The process for gaining data access should be a relatively simple

⁵ It is assumed that companies will comply with relevant breach notification laws. This is to make certain that a description of what the Customer should expect if a breach occurs is conveyed to the Customer.

106 process for the typical Customer. This process, which may include existing procedures
107 established or approved by the applicable regulatory authority or other legal
108 requirements, should be discussed in the notices to the Customer. The data provided to
109 the Customer should be provided in a form that is reasonably understandable by the
110 average Customer.

111 **Customer Authorization & Data Accuracy**

- 112 • Third Parties should provide Customers with reasonable mechanisms for:
 - 113 1. granting and revoking authorization for access to their CEUD;
 - 114 2. providing feedback regarding the disclosure of CEUD; and
 - 115 3. requesting corrections to the CEUD.

116 **Data Disclosure**

- 117 • CEUD collected by a Third Party should be limited to only that data necessary to fulfill
118 the purpose specified in the Customer's authorization⁷.
- 119 • A separate Customer authorization should be obtained before CEUD is used in a
120 materially different manner than previously authorized.

121 **Aggregated or De-identified CEUD⁸**

- 122 • If the customer has already authorized a particular service or product, and a Third party
123 or Third party's Contracted Agent needs to disclose aggregated or de-identified
124 information in order to produce that service or product, the Third Party or Third Party's
125 Contracted Agent do not need a new authorization to disclose the aggregated or de-
126 identified information so long as that information cannot be tracked back to an individual
127 or used to identify a customer.
- 128 • Third Parties should specify that any other Third Party or Contracted Agent receiving
129 CEUD that has been anonymized or de-identified should not attempt to re-identify the
130 data or otherwise identify an individual premise or Customer.

131 **Legal Disclosure for Law Enforcement**

- 132 • Third Parties should have procedures in place to provide data access to law
133 enforcement when presented with legal obligations to do so. These procedures should
134 include validation that the necessary legal requirements have been met (e.g., subpoena,
135 court order, etc.).

136 **Disclosure of Information in Situations of Imminent Threat to Life or Property**

- 137 • These practices do not apply to emergency disclosures of information provided to
138 emergency responders in situations involving an imminent threat to life or property. What
139 constitutes an emergency disclosure should be determined by appropriate authorities.

⁷ There may be a legal issue in terms of who has access to this data. There may be situations in which the Customer and the consumer are not the same and that one might want to restrict access to the CEUD. These recommended practices are not designed to determine legal issues.

⁸ There are currently no known standards for determining what constitutes de-identified CEUD. The typical intention is that all identifying information has been removed.

140 **Customer Education & Awareness**

- 141 • Third Parties should develop and implement Customer education and awareness plans
142 to inform the relevant Customers about the Third Party's CEUD privacy protection
143 policies and practices.
- 144 • The Third Party should provide its Customers with educational and awareness materials
145 that summarize the steps that the organization is taking to reduce potential risks
146 associated with unauthorized use of CEUD, and describe the steps that Customers can
147 take to help reduce their own risk.
- 148 • The customer should be made aware that CEUD may unavoidably differ somewhat from
149 different sources based on such factors as differences in technology, timing, and
150 validation. For example, potential exists that data from a HAN device may differ from an
151 aggregated view provided by a utility.

152 **Data Minimization**

- 153 • Collection of CEUD by Third Parties should be limited to only that information necessary
154 to fulfill the purpose (e.g., to provide a service or product, etc.) as set forth in the
155 Customer's authorization.

156 **Data Quality**

- 157 • Third Parties and Third Party's Contracted Agents using CEUD should endeavor to
158 ensure that the data is accurate and complete. It should be recognized that the data is
159 only as accurate and complete as the information received if the holder is not the original
160 collector. This should not preclude a Third Party or Third Party's Contracted Agents
161 from modifying or enhancing CEUD, provided that it is clear that modifications or
162 enhancements have been made when such information is disclosed.

163 **Data Security & Governance**

- 164 • Third Parties should protect information under their control from unauthorized access,
165 copying, modification, inappropriate disclosure, or loss by having information privacy
166 protections in policies, procedures, and practices relating to data security and to
167 disclosure and accuracy of data disclosed to the Third Party's Contracted Agents, or to
168 other Third Parties.
- 169 • These policies or procedures should periodically be reviewed, assessed, and updated,
170 as necessary, to ensure CEUD is properly addressed.
- 171 • Third Parties should appoint positions and/or personnel to ensure that security and
172 privacy policies are properly maintained, updated, and followed.
- 173 • Privacy practices should be transparent.

174 **Privacy Practices Risk Assessment**

- 175 • Third Parties should conduct and document periodic privacy impact and risk
176 assessments and analyses associated with their processes for disclosing CEUD to Third
177 Party's Contracted Agents. They should use these risk analyses and privacy impact

178 assessments to update, when appropriate, the applicable policies and practices. Such
179 risk analyses and privacy impact assessments should be considered at least annually or
180 when:

- 181 – Major changes occur within their organization that may reasonably impact the
182 company's data privacy practices relating to disclosing CEUD to Third Parties or
183 Third Party's Contracted Agents;
 - 184 – New applicable laws and/or regulations become effective;
 - 185 – An event related to the unauthorized disclosure of CEUD occurs at the company;
186 and
 - 187 – Any other circumstance occurs that the Third Party or Third Party's Contracted Agent
188 determines warrants such risk analysis.
- 189 • Third Party's Contracted Agents should conduct similar analyses and provide the results
190 of their analyses/assessments to the Third Party in a timely manner.
 - 191 • In developing and updating policies and practices, Third Parties should develop a set of
192 Privacy Use Cases to track information flows and the privacy implications of collecting
193 and using data to help the organization to address and mitigate the associated privacy
194 risks within common technical design practices and business practices.⁹
 - 195 • Third Parties should share solutions to common privacy-related problems with other
196 Smart Grid market participants in some appropriate manner (e.g., trade forums,
197 associations, public policy, public out-reach, external coordination, etc.).

198 **Data Retention and Disposal**

- 199 • Unless authorized differently, Third Parties should keep CEUD no longer than is
200 necessary to fulfill the business purposes for which it was collected, and as reasonably
201 interpreted to be required to comply with legal or regulatory requirements.
- 202 • If CEUD is to be used for research, then policies and procedures should be established
203 for retention and de-identification related to these activities.
- 204 • Third Parties should inform the Customers of their data retention policies as part of their
205 notice to Customers.
- 206 • Third Parties' data retention policies should include when and how data should be
207 irreversibly disposed of, including after revocation of a Customer's authorization to
208 collect or keep CEUD.

209 **Data Breaches**

- 210 • Third Parties should identify any state or federal requirements for disclosure or data
211 breach notification that may be applicable to a Third Party or Contracted Agent.

⁹ Refer to the CSWG NISTIR 7628 Use Cases here; will need a section/chapter reference.

- 212 • Consider including CEUD as data that may require a notice for any unauthorized breach
213 dependent upon the granularity of the data and applicable legal breach notification
214 requirements.

215 **Employee Training**

- 216 • Third Parties and Third Party's Contracted Agents should develop, disseminate, and
217 periodically review and update a formally documented security and privacy awareness
218 and training policy (which specifically includes the protection of CEUD) with documented
219 supporting implementation procedures.
- 220 • The organization should document, maintain, and monitor each employee's security and
221 privacy training activities on an individual basis, including basic security and privacy
222 awareness training in accordance with the organization's security and privacy policies.

223 **Audits**

- 224 • Each Third Party should conduct a periodic independent audit of Third Party's data
225 privacy and security practices.
- 226 • Each Third Party should periodically verify the privacy and security practices of Third
227 Party's Contracted Agents. This may occur in one or more ways. Some examples are:
- 228 1. Conducting an audit of the Third Party's Contracted Agents' privacy and security
229 practices.
 - 230 2. Requiring the Contracted Agent to provide Third Party with an independent audit
231 of its privacy and security practices.
 - 232 3. Examining the results of an independent audit¹⁰ of the Third Party's Contracted
233 Agents' privacy and security practices.
 - 234 4. Examine the results of a recent SSAE-16¹¹ audit.
 - 235 5. Review any existing Information Security Management System (ISMS)¹²
236 certifications.
 - 237 6. Review any recent privacy impact assessments that have been performed.

¹⁰ "Independent Audit" is described at the ISACA (previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves) site at <http://www.isaca.org/Journal/Past-Issues/2003/Volume-6/Pages/IT-Audit-Independence-What-Does-It-Mean-.aspx>

¹¹ Statement on Standards for Attestation Engagements (SSAE) No. 16 replaced the SAS70 Type II audit. "SSAE 16 is an attestation standard geared towards addressing engagements conducted by practitioners (known as "service auditors") on service organizations for purposes of reporting on the design of controls and their operating effectiveness." See more at <http://www.ssaе16.org/what-is-ssae-16/introduction-to-ssae-16.html>

¹² A certified Information Security Management System (ISMS) is described at <http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/>