Customer Service Policy A.5
Advance Metering Infrastructure (AMI) Data Security Policy

Sonoma Clean Power Authority (SCPA) understands the vital importance of ensuring the privacy and security of AMI data and customer usage information. The California Public Utilities Commission (CPUC or Commission) Decision (Decision) 12-08-045[1] extends privacy protections to customers of community choice aggregators, including SCPA. "Attachment B" of the Decision lists the rules regarding privacy and security protections for energy usage data that SCPA follows.

In compliance with "Attachment B", SCPA shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

SCPA and all SCPA contractors, consultants and other third parties who obtain access to covered information based on consent from SCPA shall provide reasonable training to all employees and contractors who use, store or process covered information as needed to comply with this Policy and CPUC rules and regulations related to AMI Data Security in accordance with "Attachment B".

Per "Attachment B", SCPA shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish SCPA's specific primary purpose.

SCPA shall comply with Decision 12-08-045, "Attachment B", including any amendments made by the CPUC. See following pages for a copy of "Attachment B".

[1] https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M026/K531/26531585.PDF

Adopted: February 7, 2019
Amended: October 1, 2020

ATTACHMENT B

ATTACHMENT B:

Rules Regarding Privacy and Security Protections for Energy Usage Data Applicable to Community Choice Aggregators or Electrical Service Providers (when providing service to residential or small commercial customers)

1. DEFINITIONS

(a) **Covered Entity**. A "covered entity" is (1) any Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers), or any third party that provides services to a Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) under contract, (2) any third party who accesses, collects, stores, uses or discloses covered information pursuant to an order of the Commission, unless specifically exempted, who obtains this information from an electrical corporation, a Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers)or (3) any third party, when authorized by the customer, that accesses, collects, stores, uses, or discloses covered information relating to 11 or more customers who obtains this information from an electrical corporation, a Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers).[1]

(b) **Covered Information**. "Covered information" is any usage information obtained through the use of the capabilities of Advanced Metering Infrastructure when associated with any information that can reasonably be used to identify an individual, family, household, residence, or non-residential customer, except that covered information does not include usage information

[1] The Commission and its agents, including but not limited to contractors and consultants, are not "covered entities" subject to these rules because the Commission and its agents are subject to separate statutory provisions pertaining to data.

from which identifying information has been removed such that an individual, family, household or residence, or non-residential customer cannot reasonably be identified or re-identified. Covered information, however, does not include information provided to the Commission pursuant to its oversight responsibilities.

(c) **Primary Purposes**. The "primary purposes" for the collection, storage, use or disclosure of covered information are to—

(1) provide or bill for electrical power or gas,

(2) provide for system, grid, or operational needs,

(3) provide services as required by state or federal law or as specifically authorized by an order of the Commission, or

(4) plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with a Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers), under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission.

(e) **Secondary Purpose**. "Secondary purpose" means any purpose that is not a primary purpose.

2. TRANSPARENCY (NOTICE)

(a) **Generally**. Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the accessing, collection, storage, use, and disclosure of covered information. Provided, however, that covered entities using covered data solely for a primary purpose on behalf of and under contract with utilities are not required to provide notice separate from that provided by the utility.

(b) **When Provided**. Covered entities shall provide written notice when confirming a new customer account and at least once a year shall inform customers how they may obtain a copy of the covered entity's notice regarding the accessing, collection, storage, use, and disclosure of covered information, and shall

provide a conspicuous link to the notice on the home page of their website, and shall include a link to their notice in all electronic correspondence to customers.

(c) **Form**. The notice shall be labeled Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information and shall—

(1) be written in easily understandable language, and

(2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice and the posted privacy policy shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice or posted privacy policy,

(3) the covered entity's process for altering the notice or posted privacy policy, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

3. PURPOSE SPECIFICATION

The notice required under section 2 shall provide—

(a) an explicit description of—

(1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed,

(2) each category of covered information that is disclosed to third parties, and, for each such category, (i) the purposes for which it is disclosed, and (ii) the categories of third parties to which it is disclosed, and

(3) the identities of those third parties to whom data is disclosed for secondary purposes, and the secondary purposes for which the information is disclosed;

(b) the approximate period of time that covered information will be retained by the covered entity;

(c) a description of—

(1) the means by which customers may view, inquire about, or dispute their covered information, and

(2) the means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access**. Covered entities shall provide to customers upon request convenient and secure access to their covered information—

(1) in an easily readable format that is at a level no less detailed than that at which the covered entity discloses the data to third parties.

(2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.

(b) **Control**. Covered entities shall provide customers with convenient mechanisms for—

(1) granting and revoking authorization for secondary uses of covered information,

(2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and

(3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process**.

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, law, or order of the Commission, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law as necessary.

(2) Unless otherwise prohibited by court order, law, or order of the Commission, a covered entity, upon receipt of a subpoena for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, in written form, and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) On an annual basis, covered entities shall report to the Commission the number of demands received for disclosure of customer data pursuant to legal process or pursuant to situations of imminent threat to life or property and the number of customers whose records were disclosed. Upon request of the Commission, covered entities shall report additional information to the Commission on such disclosures. The Commission may

make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.

(d) **Disclosure of Information in Situations of Imminent Threat to Life or Property.** These rules concerning access, control and disclosure do not apply to information provided to emergency responders in situations involving an imminent threat to life or property. Emergency disclosures, however, remain subject to reporting rule 4(c)(6).

5. DATA MINIMIZATION

(a) **Generally**. Covered entities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(b) **Data Retention**. Covered entities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(c) **Data Disclosure**. Covered entities shall not disclose to any third party more covered information than is reasonably necessary or as authorized by the Commission to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

6. USE AND DISCLOSURE LIMITATION

(a) **Generally**. Covered information shall be used solely for the purposes specified by the covered entity in accordance with section 3.

(b) **Primary Purposes**. A Community Choice Aggregator, an Electrical Service Provider (when providing service to residential

or small commercial customers), a third party acting under contract with the Commission to provide energy efficiency or energy efficiency evaluation services authorized pursuant to an order or resolution of the Commission, or a governmental entity providing energy efficiency or energy efficiency evaluation services pursuant to an order or resolution of the Commission may access, collect, store and use covered information for primary purposes without customer consent. Other covered entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here.

(c) **Disclosures to Third Parties**.

(1) **Initial Disclosure by a Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers)**. A Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers) may disclose covered information without customer consent to a third party acting under contract with the Commission for the purpose of providing services authorized pursuant to an order or resolution of the Commission or to a governmental entity for the purpose of providing energy efficiency or energy efficiency evaluation services pursuant to an order or resolution of the Commission. A Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers) may disclose covered information to a third party without customer consent

a. when explicitly ordered to do so by the Commission; or

b. for a primary purpose being carried out under contract with and on behalf of the Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers)disclosing the data; provided that the covered entity disclosing the data shall, by contract, require the third party to agree to access, collect, store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which

the covered entity itself operates as required under this rule, unless otherwise directed by the Commission.

(2) **Subsequent Disclosures**. Any entity that receives covered information derived initially from a covered entity may disclose such covered information to another entity without customer consent for a primary purpose, provided that the entity disclosing the covered information shall, by contract, require the entity receiving the covered information to use the covered information only for such primary purpose and to agree to store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the covered entity from which the covered information was initially derived operates as required by this rule, unless otherwise directed by the Commission.

(3) **Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances**. When a covered entity discloses covered information to a third party under this subsection 6(c), it shall specify by contract, unless otherwise ordered by the Commission, that it shall be considered a material breach if the third party engages in a pattern or practice of accessing, storing, using or disclosing the covered information in violation of the third party's contractual obligations to handle the covered information under policies no less protective than those under which the covered entity from which the covered information was initially derived operates in compliance with this rule.

- If a covered entity disclosing covered information for a primary purpose being carried out under contract with and on behalf of the entity disclosing the data finds that a third party contractor to which it disclosed covered information is engaged in a pattern or practice of accessing, storing, using or disclosing covered information in violation of the third party's contractual obligations related to handling covered information,

the disclosing entity shall promptly cease disclosing covered information to such third party.

- If a covered entity disclosing covered information to a Commission-authorized or customer-authorized third party receives a customer complaint about the third party's misuse of data or other violation of the privacy rules, the disclosing entity shall, upon customer request or at the Commission's direction, promptly cease disclosing that customer's information to such third party. The disclosing entity shall notify the Commission of any such complaints or suspected violations.

(4) Nothing in this section shall be construed to impose any liability on a Community Choice Aggregator or an Electrical Service Provider (when providing service to residential or small commercial customers) relating to disclosures of information by a third party when i) the Commission orders the provision of covered data to a third party; or ii) a customer authorizes or discloses covered data to a third party entity that is unaffiliated with and has no other business relationship with the Community Choice Aggregator or the Electrical Service Provider (when providing service to residential or small commercial customers). After a secure transfer, the Community Choice Aggregator or the Electrical Service Provider (when providing service to residential or small commercial customers) shall not be responsible for the security of the covered data or its use or misuse by such third party. This limitation on liability does not apply when a utility has acted recklessly.

(d) **Secondary Purposes**. No covered entity shall use or disclose covered information for any secondary purpose without obtaining the customer's prior, express, written authorization for each type of secondary purpose. This authorization is not required when information is—

(1) provided pursuant to a legal process as described in 4(c) above;

(2) provided in situations of imminent threat to life or property as described in 4(d) above; or

(3) authorized by the Commission pursuant to its jurisdiction and control.

(e) **Customer Authorization**.

(1) **Authorization**. Separate authorization by each customer must be obtained for all disclosures of covered information except as otherwise provided for herein.

(2) **Revocation**. Customers have the right to revoke, at any time, any previously granted authorization.

(3) **Opportunity to Revoke**. The consent of a residential customer shall continue without expiration, but an entity receiving information pursuant to a residential customer's authorization shall contact the customer, at least annually, to inform the customer of the authorization granted and to provide an opportunity for revocation. The consent of a non-residential customer shall continue in the same way, but an entity receiving information pursuant to a non-residential customer's authorization shall contact the customer, to inform the customer of the authorization granted and to provide an opportunity for revocation either upon the termination of the contract, or annually if there is no contract.

(f) **Parity**. Covered entities shall permit customers to cancel authorization for any secondary purpose of their covered information by the same mechanism initially used to grant authorization.

(g) **Availability of Aggregated Usage Data**. Covered entities shall permit the use of aggregated usage data that is removed of all personally-identifiable information to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

7. DATA QUALITY AND INTEGRITY

Covered entities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete or otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.

8. DATA SECURITY

(a) **Generally**. Covered entities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(b) **Notification of Breach**. A covered third party shall notify the covered Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) that is the source of the covered data within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a covered Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) or by a covered third party, the covered Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) shall notify the Commission's Executive Director of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a covered third party of such a breach. Upon request by the Commission, Community Choice Aggregators or Electrical Service Providers (when providing service to residential or small commercial customers) shall notify the Commission's Executive Director of security breaches of covered information.

(c) **Annual Report of Breaches.** In addition, Community Choice Aggregators or Electrical Service Providers (when providing service to residential or small commercial customers) shall file an annual report with the Commission's Executive Director, commencing with the calendar year 2012, that is due within 120 days of the end of the calendar year and notifies the Commission of all security breaches within the calendar year affecting covered information, whether by the covered Community Choice

Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) or by a third party.

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit—

(1) the privacy notices that they provide to customers,

(2) their internal privacy and data security policies,

(3) the categories of agents, contractors and other third parties to which they disclose covered information for a primary purpose, the identities of agents, contractors and other third parties to which they disclose covered information for a secondary purpose, the purposes for which all such information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose. (A covered entity shall retain and make available to the Commission upon request information concerning who has received covered information from the covered entity.), and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Customer Complaints**. Covered entities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

(c) **Training**. Covered entities shall provide reasonable training to all employees and contractors who use, store or process covered information.

(d) **Audits**. Each Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) shall conduct an independent audit of its data privacy and security practices in conjunction every three

years following 2012 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) shall report the findings to the Commission.

(e) **Reporting Requirements**. On an annual basis, each Community Choice Aggregator or Electrical Service Provider (when providing service to residential or small commercial customers) shall disclose to the Commission as part of an annual report required by Rule 8.b, the following information:

(1) the number of authorized third parties accessing covered information,

(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

(END OF ATTACHMENT B)

Concurrence of Commissioner Timothy Alan Simon on Item 47
Decision 12-08-045 Extending Privacy Protections to
Customers of Gas Corporations and Community Choice Aggregators,
and to Residential and Small Business Customers
of Electric Service Providers

This Decision (D.) 12-08-045 establishes Advanced Metering Infrastructure (AMI) technology privacy protections for gas customers of Pacific Gas and Electric Company, Southern California Gas Company, and San Diego Gas & Electric Company, similar to those adopted in D.11-07-056 for their electric customers. The Decision also extends privacy protections to the customers of Community Choice Aggregators (CCA) and to the residential and small commercial customers of electric service providers (ESP). These adopted rules are consistent with Senate Bill (SB) 1476 (Padilla, Stats. 2009, ch. 327), as well as California Public Utilities Code § 366.2(c) and § 394.4.[1] Finally, for purposes of this concurrence, D.12-08-045 declines to consolidate the privacy rules into a General Order, in part because of the relative infancy and untested status of the rules. I support this cautious approach to regulating the use of customer data but also have concerns on the potential chilling effects.

"Smart" wired and wireless information technologies are important conservation and market-shaping tools for critical policy objectives including, but not limited to, energy efficiency, demand response, load shifting, renewables and dispatched back-up generation, as well as, stronger protections against outages due to cyber attack or system errors. My concern is that we do not limit access to customer data to the extent that we bar existing or potential market participants who could create better energy products and services based on that analysis of this customer data. It is important to strike a balance. Otherwise, we will find the market largely dominated by a few energy providers and not our envisioned robust, competitive, and liquid market place.

Unprecedented collection of highly granular energy usage data—just short of 3000 data points per month from a smart meter collecting data every quarter-hour—allows anyone with access to that data to observe variations in consumption that can reveal household activities such as whether homes are occupied, which appliances and devices are being used, whether an alarm system is activated, as well as work schedules and traveling patterns. Our challenge is to balance having enough granular data to make it useful for innovation, while protecting individual privacy and public safety. Giving customers' confidence that their data is secure encourages acceptance of new technologies.

[1] SB 1476 prohibits electrical and gas corporations from disclosing customer usage data to third parties, except as authorized, and prevents subject utilities, CCAs and ESPs from offering incentives or discounts for allowing access to that data. I commend Senator Padilla for striking a balanced approach to data privacy and competitive markets.

The growth of human behavioral economics, as a method of developing competitive applications, has an amazing future potential in the energy markets. We have seen an early glimpse in advance metering infrastructure and demand response but clearly not to the extent that we could with more competitive access to usage data. Recently in the European Union I experienced direct smart phone marketing leveraging location data improving purchasing power with vendors offering sales at certain slower demand times. This same ingenuity will benefit energy consumers as there data and time of use pricing is aggregated to forecast with other factors energy market demand and capacity. I know from my experience as a banking and securities attorney that in the financial services sector market access to consumer data is executed in omnibus or aggregated forms. These applications can result in more market competition and consumer choice; while protecting the names and other sensitive data points the customers may prefer remain private.

Excessive protection of customer data typically benefits the industry incumbents who possess the data. Our Orwellian fears of Big Brother are relics of the past. Privacy was something we experienced long before we used the various new electronic communications technologies, like credit card payments and airline reservation systems, which establish our locations and reveal our lifestyles. To expect energy markets to be insulated from this reality is anticompetitive.

Similarly, applications and devices to help consumers manage and understand the environmental impacts of their energy use are also ripe for innovation. Bright young companies are aiming to provide not only smart grid software services for utility operations, but smart meter data services using individual customer data. Additionally, new methods for two-way communication between the utility or third party and the customer--home area network (HAN) devices that communicate over the Internet through a web portal or through the utility's advanced metering infrastructure (AMI) network will help customers monitor their usage and alert them to grid shortages. New ways of connecting smart devices directly to the grid through Internet or AMI networks allow customers to analyze their usage by appliance category as well as time of use, and to control them both manually and automatically. New social media applications could allow individuals to compete with online friends to save energy and lower carbon emissions. Companies are already developing online and mobile applications for businesses and consumers that can use "Green Button" data to help consumers choose the most economical rate plan, deliver customized energy-efficiency tips, provide tools to size and finance rooftop solar panels, or conduct virtual energy audits.[2] These new market

[2] The Obama Administration's Green Button initiative, launched in January, aims to foster innovation in online energy management tools through their "Green Button" initiative. Utilities and electricity suppliers will allow customers to download their own household or building energy-use data in a secure, user-friendly format with a click of an online "Green Button." Participating utilities have agreed to base their Green Buttons on a common technical standard, which will allow software developers and other entrepreneurs to leverage enough users to support the

Footnote continued on next page

entrants will not want to rely on smart meter data provided by utility back offices but will want access the data directly from the customer.

In conclusion, our rules recognize that consumer protection means giving customers control over their data and also allowing them to share it if they choose. D12-08-045 strikes the proper balance between protecting customers' right to privacy and not giving incumbents a competitive advantage. I concur with this Decision as an important step to striking the balance between privacy rights and the need for access to relevant energy data. I also encourage this Commission to look closely at best practices that protect sensitive data while promoting innovative energy products and services that ultimately will benefit consumers with choice.

Dated August 31, 2012, San Francisco, California

/s/ TIMOTHY ALAN SIMON
Timothy Alan Simon
Commissioner

creation of new applications that can help consumers. According to a March 2012 White House press release, companies who are developing applications using the Green Button standard include Belkin, Efficiency 2.0, EnergySavvy, FirstFuel, Honest Buildings, Lucid, Plotwatt, Schneider-Electric, Simple Energy, and Sunrun. Companies who have deployed or who support deployment of Green Buttons include Aclara, Tendril, PG&E, SDG&E, SoCal Edison, Oncor, Itron, OPower, Oracle, and Silver Spring Networks.