DOCKETED

Docket Number:	16-OIR-03
Project Title:	Energy Data Collection
TN #:	221263
Document Title:	SMUD Comments on Data Collection Rulemaking Express Terms
Description:	N/A
Filer:	System
Organization:	SMUD
Submitter Role:	Public Agency
Submission Date:	9/20/2017 3:53:30 PM
Docketed Date:	9/20/2017

Comment Received From: Steven G. Lins
Submitted On: 9/20/2017
Docket Number: 16-OIR-03

Comments on Data Collection Rulemaking Express Terms

Comments of the Sacramento Municipal Utility District on Data Collection Rulemaking Express Terms.

Additional submitted attachment is included below.

STATE OF CALIFORNIA
BEFORE THE CALIFORNIA ENERGY COMMISSION

In the matter of:	)	Docket No. 16-OIR-03
	)	
Developing Regulations, Guidelines, and Policies for Implementing SB 350 and AB 802	)	SMUD Comments On Data Collection Rulemaking Express Terms
	)	
	)	September 20, 2017

Comments of the Sacramento Municipal Utility District on Data Collection Rulemaking Express Terms

Thank you for the opportunity to provide comments on the Data Collection Rulemaking Express Terms ("Express Terms"), intended to update the California Energy Commission's ("CEC") Title 20 data collection regulations to support the implementation of Senate Bill 350 ("SB 350"), Assembly Bill 802 ("AB 802"), and improved energy analytics at the CEC.

SMUD appreciates the opportunities CEC staff has provided for stakeholder feedback, and SMUD believes this iterative process has been helpful. Sections 1306(a)(5) and 1306(c)(3) are useful additions to avoid and reduce duplicative reporting requirements.

While many of SMUD's requested changes and clarifications have been addressed, there are a few remaining concerns that SMUD would like to present in these written comments. We thank the CEC in advance for their consideration.

Section 1304(b): SMUD reiterates its previous comment expressing concerns about Utility Distribution Company ("UDC") reporting of data on power plants with no minimum size, rather than the current 100 kilowatt (kW) and above structure. First, much of the list of data required in these reports, while available generally for systems of 100 kW or greater, are not available for smaller systems. For example, for residential sized solar systems or storage systems there will be:

- No "name";
- No facility code assigned by the Energy Information Administration;
- A question about whether facility owner's full legal name and address should be provided for residential systems, and a question about what is meant by "principal place of business" in this context;
- A general lack of information with respect to dates of disconnection of these systems.

Second, the inclusion of energy storage systems is premature, given the small penetration of these resources. For example, while there are a handful of SMUD customers with small photovoltaic (PV) integrated battery storage, none are designed to export to the utility. SMUD has received applications for some "non-export" behind-the-

meter PV systems with storage, but these small battery systems are no different than the other thousands of behind-the-meter uninterruptible power supplies ("UPS") those utility customers, such as data centers, have been using for decades. Furthermore, utility knowledge of storage systems installed by residential customers, as well as their disconnection, is not guaranteed, nor necessarily common. Until the technology and economics of these storage systems advances, requiring the detailed reporting as outlined in this section is unduly burdensome and inefficient.

SMUD suggests that Section 1304(b) remain applicable only to power plants 100 kW in size or above. Understanding that the CEC desires to have better data on the rising number of smaller distributed energy resources, including storage resources, SMUD suggests that a new Section 1304(c) be created that requests applicable and available data and/or reports on systems smaller than 100 kW. Data that may be considered applicable could include nameplate, address, operating mode, technology type, interconnection date, and perhaps service account, premise, meter, and rate information. Unless the CEC intends to include back-up generators, it is almost certain that fuel type will not be useful, as that will be indistinguishable from technology type.

SMUD notes that not all UDCs may have the applicable data available as a matter of course. Hence, SMUD suggests that a statement similar to that in Section 1353(a)(2) be included, stating: "No entity subject to reporting requirements pursuant to this Section shall be required to provide data or reports that it does not collect in the regular course of business; however, if the entity begins to collect some or all of the data not previously collected, it must submit the data in accordance with the requirements of this section."

Section 1353: The new Section 1353 of the Express Terms represents a vast expansion of data to be reported for UDCs, including monthly sales for each customer, as well as detailed information for each of these customers. SMUD has previously expressed concern that this level data is not necessarily available to the UDCs, would increase costs tremendously, and may not be more beneficial than aggregated data. However, SMUD understands the CEC has remained consistent in the type of data expansion it seeks. Therefore, SMUD requests that given UDC concerns about what information is available to report, the CEC should convene a working group to help understand what kind of data is available, how robust the availability is, how easy or difficult it is to collect and include such data, and what the CEC actually needs in order to produce better forecasts and serve other projects of interest.

Additionally, SMUD still has concerns regarding confidentiality of such detailed customer information. At SMUD, we require an industry standard annual report from our vendors that store SMUD data, called an SSAE16 or something similar, which is a report produced from an independent 3rd party assessment/audit of the company's security controls and program. SMUD also requires vendors to submit a self-produced System Security Plan (see Attachment A) to provide assurance that the security controls employed in protecting the data to be shared are commensurate with the level of sensitivity of the data. Since the CEC will be increasing the amount of customer information it will be storing, it would be helpful for the CEC to confidentially share an

SSAE-16 audit report or a system security plan with us annually so we have visibility into the CEC's information security and privacy programs. At the very least, CEC should certify their information security and privacy programs are compliant with California law, and all applicable State of California information security and privacy policies and standards. As such, SMUD requests that UDCs only be required to provide aggregated data, and any aggregated data shared be contractually or technically restricted from re-identification.

Sections 1308, 1314, and 1353: In Sections 1308, 1314, and 1353, there are proposed provisions for natural gas utilities and pipelines that deliver more than 200 million therms of natural gas annually. Technically, SMUD appears to meet the definition of "gas utility" because it delivers more than 200 million therms annually to our four power plants that are owned and operated by joint powers authorities (JPAs). SMUD sells gas to no other customers. Thus, SMUD is in a unique situation, unlike the common understanding of a gas utility that has retail end-use customers. In discussions with CEC staff, it has been made clear the intent of these provisions is not to include SMUD in the definition of "natural gas utility if that exclusion does not lead to 'gaps' in the natural gas data being requested." In other words, if the gas data requested is reported by another entity, CEC staff does not intend for it to be collected as well from SMUD. SMUD will continue to work with CEC staff to understand the need, or not, for SMUD to report under these provisions and would appreciate written language that clarifies SMUD's reporting responsibilities.

Thank you again for the opportunity to comment on the Express Terms.

/s/

STEVEN G. LINS
Chief Assistant General Counsel
Sacramento Municipal Utility District
P.O. Box 15830, MS A311
Sacramento, CA 95852-0830

/s/

TIMOTHY TUTT
Program Manager, State Regulatory Affairs
Sacramento Municipal Utility District
P.O. Box 15830, MS A313
Sacramento, CA 95852-0830

cc: Corporate Files (LEG 2017-0483)

ATTACHMENT A:
SMUD'S SYSTEM SECURITY PLAN

Contractor must develop and maintain a System Security Plan (SSP) that contains, at a minimum, the components listed below. The SSP must be approved by the SMUD Contract Manager and Information Security Office prior to awarding of the contract Scope of Services.

The Contractor must notify SMUD within 30 days of any system or procedural change that changes the contents of a previously approved SSP. The SSP must also be updated upon SMUD request and resubmitted to SMUD Contract Manager and Information Security Office. This document will be marked and treated as a Sensitive and Confidential document. Only authorized Contractor and SMUD staff will have access to view this document.

1. **Information Security Program**: this section must contain a description of the size of the Information Security team and their relationship to the officers of the organization. Include descriptions of the certifications and qualifications of the Information Security staff. Include information on the Information Security policies, standards and procedures that are in place, the last time they were updated, and who approves their adoption.

2. **Security Development Lifecycle**: this section must contain information on the security development lifecycle; how security is integrated into each step of the software and system development lifecycle. Include any security training that application developers have completed or are required to complete.

3. **System Architecture**: this section must contain the written description of the architecture for all systems that will be used to meet the Scope of Services under this contract. Include network and system diagrams that depict the written description.

4. **Application Architecture**: this section must contain a written description of the application that shows how the data flows between systems, the ports and services that are used, and data interfaces. The components of this section must either be depicted in Application specific diagrams or they can also be included in the System Architecture diagrams.

5. **Authentication, Authorization and Accounting (AAA) services**: this section must contain the methods used to implement AAA services throughout the system and application architecture. Include a description of where credentials are stored, how they are stored, the process to provision and revoke access, default accounts, and role-based access capabilities to the systems, where system logs are stored, and how system logs are reviewed for identifying security events.

6. **Data Exchanges**: this section must contain the technical methods and procedures for securely transmitting data between systems and entities.

7. **Data Storage**: This section must contain the technical methods and procedures for securely storing SMUD data within your system or application.

8. **Session Handling**: for web based applications this section must contain the methods used to perform session handling within the application, how returning customers are recognized, and how sessions will be transferred and authenticated between the SMUD customer portal “Your Account” and the applications that are part of the Scope of Services, if applicable.

9. **System Logging**: this section must contain the methods used to generate, maintain and analyze system activity logs for security, auditing, and troubleshooting purposes. Identify the types of logs that will be available, including success/failure events, how logs are reviewed by Contractor and incidents are communicated to SMUD, and how the logs will be made available to SMUD technical staff for review and (for SMUD hosted solutions) how logs could be exported to a SMUD Security Event Information Management solution. Include log retention periods in response.

10. **Incident Management**: this section must contain the methods used to respond to an incident, including how incidents are communicated to SMUD, and how the logs will be made available to SMUD technical staff for review and (for SMUD hosted solutions) how logs could be exported to a SMUD Security Event Information Management solution. Include log retention periods in response.

11. **Vulnerability Management Program**: this section must contain the methods used to implement a Vulnerability Management Program for antivirus, antispyware, security patch management, secure coding practices, testing for website vulnerabilities (i.e. cross site scripting and SQL injections), session hijacking, session replay attempts and buffer overflow attempts. Include information on any third-party assessments that have been performed, how often they are performed and who performs them. SMUD may request to review the findings from the assessments and may perform our own vulnerability assessment prior to contract award.

12. **System and Data Recovery Program**: this section must contain the methods to recover the systems and applications that are required under the Scope of Services. Identify the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) your system is able to support. Include onsite and offsite backup processes (i.e. disk-to-disk, tapes), backup schedules, tape rotations, and disaster testing processes.

13. **Change Control Process**: this section must contain the methods used to document, test and implement changes to the systems and applications being provided under the Scope of Services.

14. **Physical Security Program**: If the solution will not be hosted by SMUD, this section must contain the methods used to protect the physical security of the infrastructure, applications and systems under the Scope of Services. Include the physical address of the Data Center, physical access control processes, identity identification process, physical access authorization and revocation processes.

15. **Audits and Assessments**: For any non-SMUD hosted system, provide the SMUD Information Security Office and Audit and Quality Services Office a copy of the Statement on Standards for Attestation Engagements Number 16 (SSAE16) report (formerly known as the Statement of Auditing Standards Number 70 (SAS70) report), Payment Card Industry Data Security Standard (PCI DSS) certification, or other comparable independent assessments and/or certifications. In addition, annual updates to these reports must be provided as they are made available.