Company: San Diego Gas & Electric Company (U902M)
Proceeding: 2016 General Rate Case
Application: A.14-11-___
Exhibit: SDG&E-38

SDG&E

DIRECT TESTIMONY OF GREGORY D. SHIMANSKY

(COMPLIANCE)

November 2014

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

SDGE
A Sempra Energy utility®

TABLE OF CONTENTS

SUMMARY

- This testimony provides a status on compliance items that are to be reported in this Test Year 2016 General Rate Case Application for SDG&E, pursuant to the Commission's Rate Case Plan. Specifically, my testimony reports on compliance items stemming from SDG&E's 2012 GRC decision (D.13-05-010), and compliance items stemming from other regulatory decisions.

SDG&E DIRECT TESTIMONY OF GREGORY D. SHIMANSKY (COMPLIANCE)

I. INTRODUCTION

A. Summary of Process

My testimony presents a list of the GRC compliance items that the Commission has either ordered SDG&E to perform or that have been agreed to by SDG&E in settlement, as adopted by the California Public Utilities Commission ("CPUC" or "Commission"). The Commission's Rate Case Plan ("RCP")[1] governs filing dates, revision dates, and time schedules for the major investor-owned utility GRC proceedings. Pursuant to the RCP, my testimony provides a status on whether SDG&E has performed "all studies and information required to be submitted in the rate case by the Commission in prior rate decisions and subsequent policy statements of decisions."[2]

The primary GRC compliance items are found in the Commission's Ordering Paragraphs ("OPs") in Decision ("D.) 13-05-010, its decision adopting the Test Year 2012 GRC for SDG&E (hereinafter, "TY2012 GRC Decision"). In addition, I conducted a review of other Commission decisions and currently ongoing regulatory proceedings for potential compliance items requiring the submission of studies or information in this GRC.

B. Organization of Testimony

Based on the review process described above, this testimony provides a list of compliance items, and provides the following information: the source of the requirement / obligation, a description of the nature of the item, the actions performed, and the status of each compliance item.

My testimony is organized as follows:

- Section II provides information regarding the obligations and / or commitments of SDG&E broken into related categories:
    - Revenue Requirement filings and Results of Operations from D.13-05-010.
    - Memorandum of Understanding ("MOU") with the Center for Accessible Technology ("CforAT") from D.13-05-010.

[1] *See* D.07-07-004, D.04-12-015 and D.89-01-040.
[2] *See* D. 07-07-004, Appendix A, p. A-32.

- Account change requirements relating to D.13-05-010.
- Required reports and studies.
- Other topics.

II. COMPLIANCE ITEMS, OBLIGATIONS, AND COMMITMENTS

The following list of SDG&E compliance items was developed according to the review described in Section I.A. The items are organized according to the following categories (in sequential order): Revenue Requirement and Results of Operations, MOU with CforAT, Account Changes, Required Reports, and Other.

A. Revenue Requirement and Results of Operations

1. Implement test year base margins for gas and electric service consistent with the values the Commission approved in the TY2012 GRC, and represented in the RO Model for TY2012.

   - Source: TY2012 GRC Decision, OP 3 and Page 2
   - Requirement: "The adopted adjustments, after inputting them into the Results of Operations model, result in the revenue requirements shown in Attachment B of this decision, which are adopted. A.) For San Diego Gas & Electric Company, the adopted combined gas and electric test year 2012 revenue requirement is $1,732,830,000."
   - Action Performed: SDG&E submitted Advice Letter ("AL") 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The electric service base margin value is referenced in the Electric Rates section at page 2. The gas service base margin value is referenced in the Gas Rates section at page 3. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4.
   - Status: Completed.

2. Implement base margins for attrition years 2013, 2014, and 2015 for gas and electric service consistent with the authorized percentage growth allowed over the TY2012 base margin values the Commission approved in the TY2012 GRC.

- Source: TY2012 GRC Decision, OP 4
- Requirement: "The post-test year attrition adjustments of 2.65% for 2013, 2.75% for 2014, and 2.75% for 2015 is adopted, and San Diego Gas & Electric Company shall use those post-year adjustment percentages to adjust… test year 2012 revenue requirement for 2013, 2014, and 2015."
- Action Performed: For 2013, SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The electric service base margin attrition percentage is referenced in the Electric Rates section at page 2. The gas service base margin attrition percentage is referenced in the Gas Rates section at page 3. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4.
  - For 2014 post-test year, SDG&E filed ALs 2564-E / 2258-G the Consolidated Filing to Implement January 1, 2014 Electric and Gas Rates, and AL 2535-E the Annual Non-Fuel Generation Balancing Account Update. These amounts are consistent with D.13-05-010.
  - 2015 post-test year margin numbers have not been filed yet.
- Status: Completed.

3. Within 15 days, file Tier 1 AL, including revised tariff sheets, to implement the authorized revenue requirements in the GRC.

- Source: TY2012 GRC Decision, OP 5 and Page 81
- Requirement: "Within 15 days from the effective date of this Order, San Diego Gas & Electric Company shall file a Tier 1 Advice Letter, with revised tariff sheets, to implement the 2012 and 2013 revenue requirement authorized by OP 3 and OP 4 of this Order. The revised tariff sheets shall (a) become effective on September 1, 2013, subject to a finding of compliance by the Commission's Energy Division and (b) comply with General Order 96-B."

- Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013, within 15 days of the May 9, 2013 decision date. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The revised tariff sheets can be found in Attachment B of the ALs. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4.
- Status: Completed.

4. GRC Memorandum Account ("GRCMA") amortization.

- Source: TY2012 GRC Decision, OP 5b. and pages 81, 995, 996.
- Requirement: "The balances recorded on SDG&E's General Rate Case Revenue Requirement Memorandum Account from January 1, 2012 until the effective date of the new tariffs required by this order, shall be amortized in rates beginning September 1, 2013 through December 31, 2015."
- Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013, within 15 days of the May 9, 2013 decision date. On August 12, 2013, SDG&E filed a Supplemental AL (AL 2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The electric portion of the memo account (GRCMA) to be amortized is on page 2 of the AL and the gas portion is on page 3. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4. Further, SDG&E filed annual regulatory account update advice letters, one for Electric (AL 2532-E) and one for Gas (AL 2237-G), in late October 2013 for approval to include the 2014 portion in January 1, 2014 rates (figures found on Attachment A of the respective ALs). Also, on October 31, 2014, SDG&E filed AL 2664-E and on October 29, 2014, SDG&E filed AL 2332-G to include the 2015 portion for electric and gas, respectively, into rates on January 1, 2015.
- Status: Completed.

5. SDG&E's portion of the SONGS base margin from Southern California Edison's GRC (D.12-11-051).

- Source: TY2012 GRC Decision, OP 6 and Conclusion of Law 7.
- Requirement: "Within 15 days from the effective date of this Order, San Diego Gas & Electric Company shall file a Tier 1 Advice Letter to reflect its share of the preliminary allowance of the 2012 San Onofre Nuclear Generating Station operations and maintenance costs, and capital costs, as set forth in Decision 12-11-051."
- Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September

1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The San Onofre Nuclear Generating Station base margin value is referenced in the Electric Rates section at page 2. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4.

- Status: Completed.

6. The TY2012 GRC decision requires SDG&E to file a rate case for TY 2016.

   - Source: TY2012 GRC Decision, OP 27 and Conclusion of Law 69.
   - Requirement: "San Diego Gas & Electric Company … shall file (its) respective test year 2016 general rate case application beginning with (its) respective Notice of Intent in August 2014."
   - Action Performed: SDG&E tendered its NOI on July 25, 2014, consistent with, and slightly ahead of, the timing identified in the Commission's adopted RCP per D.93-07-030, which would be sufficient for a Test Year 2016 GRC Application.
   - Status: Completed with the acceptance of the SDG&E GRC Application filing.

7. The TY2012 GRC decision accepts SDG&E's proposal to keep rates low for ratepayers by removing our request for working cash in the application.

   - Source: TY2012 GRC Decision, at page 13.
   - Requirement: "request zero funding for each Applicant's working cash requirement in test year 2012. This proposal will have the effect of excluding the working cash requirement from rate base, and earning a rate of return."
   - Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. Pursuant to the approved decision in the TY 2012 GRC, the SDG&E RO model was adjusted to remove the working cash request, resulting in zero funding associated with that account.
   - Status: Completed.

8. The TY2012 GRC decision orders that SDG&E remove O&M associated with legacy meters in the magnitude of $18.9M before future year attrition is applied. This will make sure the money for legacy meters does not get attrition in post-test years like other SDG&E margin and O&M dollars.

- Source: TY2012 GRC Decision, at Page 918.
- Requirement: "SDG&E shall reduce its test year 2012 authorized electric distribution expenses shown in the summary of earnings tables in Attachment B of this decision by $18.9 million before it escalates electric distribution O&M expenses."
- Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. Pursuant to the approved decision in the TY 2012 GRC, the SDG&E RO model was adjusted to remove the $18.9 million before escalation was applied. Further, the Consolidated Filing (AL 2564-E) filed on December 30, 2013, shows Attrition for 2014 on the table on page 7 that has this $18.9 million adjustment.
- Status: Completed.

B. Center for Accessible Technology Memorandum of Understanding

On February 24, 2012, SDG&E, SoCalGas, and CforAT filed a joint motion in the 2012 GRC proceeding (A.10-12-005) to adopt their settlement. The settlement, known as the Memorandum of Understanding, or "MOU", was an agreement on mutually acceptable outcomes to certain access issues. In that MOU, SDG&E agreed to certain efforts such that our Branch Offices and third party payment locations are accessible, and to improve certain customer communication.

OP 1 of D. 13-05-010, approved the MOU as follows: "The February 24, 2012 joint motion, filed by the Center for Accessible Technology, San Diego Gas & Electric Company, and Southern California Gas Company, requesting that the Memorandum of Understanding between these three entities attached to that joint motion be approved and adopted."

Below, I present the status of SDG&E's ongoing efforts to meet the terms of the MOU at the time of the filing of its Test Year 2016 GRC Application.

1. Branch Offices and Authorized Payment Locations.

   - Branch Offices - Engage a Consultant to survey 1/3 of the Branch Offices following barrier removal and SDG&E will take steps to promptly remedy barriers identified. SDG&E will ensure that all newly purchased self-service kiosks will be enabled to provide audio instructions for Vision Disabled customers.
     - Result – Information relating to the satisfaction of this item can be found in the Annual Report sent to CforAT on December 6, 2013.
   - Authorized Payment Locations ("APL") – SDG&E will continue to engage a Consultant to sample 10% of their APL's annually for the duration of this MOU.
     - Result – Information relating to the satisfaction of this item can be found in the Annual Report sent to CforAT on December 6, 2013.

2. Effective Communications.

   - Utilities' Websites – Consultant to survey SDG&E's websites annually for the duration of the Compliance Period starting in 2012. Results shall be provided to CforAT in the Annual Report. SDG&E will continue to offer accessibility training to their employees engaged in website development. SDG&E will post information on their website advising customer how to obtain assistance in the event an individual with a Vision Disability experiences problem accessing documents. All new PDF documents posted on the website will be in an accessible format. After 6 months SDG&E will remove unnecessary documents that are inaccessible.

SDG&E will report the number of documents converted, remaining to convert, and those not able to convert in the Annual Report.

- Results – SDG&E has worked with CforAT on auditing "SDGE.com" for compliance with accessibility standards and is currently upgrading the site accordingly. The "myaccount.sdge.com" site is currently undergoing redeveloping and is working with CforAT on accessibility compliance. PDF files being posted are formatted to be accessible, and SDG&E has undergone a project to update historical PDF files. Finally, SDG&E continues to work with 3rd party vendors to see that their software meets accessibility standards. SDG&E expects to file an annual report by the end of 2014.

- Emergency Customer Communication System - SDG&E will continue to test its system regularly, and take any necessary action after each test. SDG&E will continue to gather information from new and existing medical baseline/life support ("MBL") customers to determine their preferred means of contact. SDG&E will also conduct outreach to elderly or disabled in its service territory in order to invite people to contact the utility and provide information on preferred method of contact.

  - Result: The outbound dialer used for emergency customer communication is tested daily at 7:00 am and a full-scale test is performed on a quarterly basis. Any problems that are identified as a result of testing are remedied.

  - In 2010, SDG&E mailed postcards to existing Medical Baseline/Life Support customers requesting the preferred method of contact for emergency notifications. The database that maintains the contact information was updated to reflect any changes that were received. In addition, the Medical Baseline enrollment application was updated to capture the preferred method of contact for new enrollments going forward.

  - SDG&E customer Solutions Outreach team works with community-based organizations in its service territory, providing them with information pertaining to emergency notification preferences. An annual workshop/training is conducted with nearly 50 nonprofit organizations serving the high risk fire areas where information related to emergency notification preferences is provided. Materials providing information on Customer Assistance offerings are available in large font and Braille.

  - SDG&E's internal system, CISCO, gets updated with the information entered in the MBL database for individual metered customers.

- Written Communications – SDG&E will study the feasibility of providing key information in large print (14 point sans serif font) on its written notices beginning with the highest priority written notices sent to customers.

- Results - Completed.

3. Pedestrian Right of Way.

- Revised Construction Standards – Pedestrian pathways will be added to the programs and SDG&E will ensure that all new employees who participate in construction work in Pedestrian Rights of Way receive training including pedestrian right of way accessibility standards.
  - Result – On the gas operations side of the business, Temporary Pathways for Public Access has been added to the SDG&E Mandatory Annual Review Training. In addition, new employees, who will be working in gas operations, are provided with, and receive training on, the Gas Operations Standard for pedestrian access requirements related to construction sites. On the electric operations side of the business, training on the electric standards regarding pedestrian rights of way has yet to be incorporated in a similar manner. SDG&E is working towards resolving this with the goal of satisfying this requirement in the upcoming months.
- Utility Poles in Pedestrian Rights of Way – For all new utility poles located in Pedestrian Rights of Way, SDG&E agrees to install such poles in a location that preserves a path of travel at least 36 inches wide, or where that is not possible, a path of travel that is at least 32 inches wide.
  - Result – SDG&E's Construction Standards and Design Manual account for this. In cases where poles need to be replaced in a sidewalk where there is no 36 inch wide path of travel, the poles are to be replaced in-kind.
- Coordination with Local Governments – SDG&E agrees to submit an advice letter to the CPUC requesting an amendment to the Utilities' Electric Rule 20A that will add wheelchair access as a consideration under that tariff within 60 days of the approval date of the final decision in D.13-05-010.
  - Result – On July 24, 2014, SDG&E filed AL 2625-E revising Electric Rule 20.a. On August 18, 2014 AL 2625-E was approved effective July 24, 2014. SDG&E acknowledges that the 60-day window for submittal had passed and SDG&E contacted CforAT upon learning of the oversight. It is now resolved.

4. Reporting and Implementation.

- Annual Reports – SDG&E will provide an Annual Report to CforAT on or about January 31st of the year following each agreement year. Each Annual Report will document all required information regarding implementation efforts that took place during the prior calendar year.
  - Result: SDG&E submitted the annual report on December 6, 2013 and plans to file the upcoming annual report around the December 2014 timeframe.

C. Required Reports and Studies

1. File, with the Directors of the Safety and Enforcement Division and the Energy Division, a semi-annual Gas Transmission and Distribution Safety Report beginning July 1, 2013.

   - Source: TY2012 GRC Decision, OP 10.
   - Requirement: "As set forth below, San Diego Gas & Electric Company (SDG&E) shall be required to serve a semi-annual Gas Transmission and Distribution Safety Report (Safety Report) on the Directors of the Safety and Enforcement Division and the Energy Division. SDG&E shall serve its first Safety Report beginning July 1, 2013, and the initial period covered by the Safety Report shall cover the one year period from January 1, 2012 through December 31, 2012. Each subsequent Safety Report shall cover each subsequent six-month period, and the second semi-annual Safety Report shall be served on September 1, 2013, and on each March 1 and September 1 thereafter until further notice."
   - Action Performed: Completed for calendar years 2012 and 2013. Ongoing requirement for 2014 and thereafter until further notice.
   - Status: Completed for calendar years 2012 and 2013. Ongoing requirement.

2. Specifically, SDG&E is required to submit data in its next GRC relating to Response to A1 Leak Orders.

   - Source: TY2012 GRC Decision, Conclusion of Law 32.
   - Requirement: "SDG&E [and SoCalGas] shall be required to compile the same type of monthly and annual data as shown on page 65 and 66 of Exhibit 145 and to supply that information in its next GRC filing."
   - Information satisfying this requirement can be found in the testimony of witness Sara Franke (Ex. SDG&E-13).
   - Status: Completed.

3. SDG&E is required to explain the efforts they have undertaken to minimize delays in responding to A1 leak orders.

   - Source: TY2012 GRC Decision, Conclusion of Law 33.
   - Requirement: "SDG&E [and SoCalGas] shall each explain in their next GRC filings what efforts they have taken to minimize delays in responding to A1 leak calls."
   - Action Performed: Information satisfying this requirement can be found in the testimony of Sara Franke (Ex. SDG&E-13).

     Status: Completed.

D. Account Change Requirements relating to D.13-05-010

1. Pensions and Post-Retirement Benefits other than Pensions Balancing Accounts.

- Source: TY2012 GRC Decision, Pages 13-14; Conclusion of Law 45, 46, and 48.
- Requirement: "The requests of SDG&E and SoCalGas to continue their two-way balancing account treatment for their respective pension benefits and PBOP costs should be granted." . . . "The requests of SDG&E and SoCalGas to continue their annual amortizations of their respective pension balancing accounts and PBOP balancing accounts should be granted." . . . "The proposal of SDG&E and SoCalGas to use the 2009 recorded costs for the PBOP for test year 2012, subject to recovery through the two-way balancing account, should be granted."
- Action Performed: SDG&E submitted AL 2485-E / 2198-G (Test Year 2012 General Rate Case (GRC) Rate Implementation Effective September 1, 2013) on May 24, 2013. On August 12, 2013, SDG&E filed a Supplemental AL (AL 2485-E-A / 2198-G-A) replacing in its entirety SDG&E's AL 2485-E / 2198-G. The AL filing shows the calculated revenue requirement associated with the final approved 2012 GRC. Inside that revenue requirement are the expenses related to Pension and PBOP's adhering to the approval to fund at 2009 recorded levels. The revenue requirement associated with Pensions at the 2009 recorded level was $18.5 million and the revenue requirement associated with PBOPs at the 2009 recorded level was $7.7 million. The Tier 1 ALs were effective as of September 1, 2013 as referenced at page 4.
  - The Pension and PBOP balancing account was not closed during the implementation of the 2012 GRC and remains open as a two-way balancing account. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the Pension and PBOP balancing accounts.
- Status: Completed.

2. Market Redesign Technology Upgrade Memorandum Account ("MRTUMA")

- Source: TY2012 GRC Decision, Page 35.
- Requirement: "With regard to SDG&E's request that its MRTUMA account should be terminated, that request should be addressed in A.11-06-003, where SDG&E is seeking recovery of its 2010 MRTU costs, or in a proceeding that covers any remaining MRTU-related costs that were recorded in 2011."
- Action Performed: On May 31, 2013, SDG&E submitted Application ("A.") 13-05-016, Application of San Diego Gas & Electric Company for Approval of ERRA Compliance for 2012 and Rate Recovery of ERRA-Related Accounts. SDG&E requests that the MRTUMA be eliminated

from SDG&E's preliminary statement on a going-forward basis. See Ex. SDG&E-35 (Jasso). SDG&E is anticipating a ruling on A.13-05-016 and has not closed the MRTUMA account.

- Status: Pending. [3]

3. New Environmental Regulations Balancing Account ("NERBA").

   - Source: TY2012 GRC Decision, OP 14; Conclusion of Law 9; and Pages 95, 249.

   - Requirement: "SDG&E is authorized to establish a two-way balancing account called the New Environmental Regulatory Balancing Account. A.) SDG&E shall file a Tier 2 advice letter within 45 days of the effective date of this decision to establish this balancing account."

   - Action Performed: SDG&E submitted AL 2496-E / 2205-G (Establishment of the New Environmental Regulatory Balancing Account Pursuant to D.13-05-010.) on June 24, 2013, within 45 days from the decision date on D.13-05-010. That AL was approved by the Energy Division on October 28, 2013, effective July 24, 2013.

     - The NERBA is still in effect. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the NERBA.

   - Status: Completed.

4. Tree Trimming Balancing Account ("TTBA").

   - Source: TY2012 GRC Decision, Page 153.

   - Requirement: "Regarding SDG&E's request to treat tree trimming costs in a two-way balancing account, we do not grant that request. By continuing the one-way balancing account at the authorized funding amount, this will encourage SDG&E to perform the needed tree trimming activities, while containing costs. SDG&E can raise its request for two-way balancing account treatment in its next GRC."

   - Action Performed: SDG&E has continued its TTBA in the same one-way balancing account fashion as prior to the 2012 GRC.

     - The TTBA is still in effect. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the TTBA. Please also refer to the Direct Testimony of Jonathan Woldemariam (Ex. SDG&E-10) for a discussion on the on-going treatment of the TTBA beginning in 2016.

   - Status: Completed.

5. Energy Storage Balancing Account ("ESBA").

[3] Application 13-05-016 is still an open proceeding and has no final decision. Therefore, SDG&E is unable to close the MRTUMA at this time.

- Source: TY2012 GRC Decision, OP 16; Findings of Fact 73; and Page 226.
- Requirement: "SDG&E is authorized to establish a one-way balancing account to record the spending of the authorized funds for energy storage projects during test year 2012 and the post-test year period. SDG&E Shall file a Tier 2 Advice Letter within 45 days of the effective date of this decision to establish this balancing account. SDG&E shall file a Tier 3 Advice Letter by November 1, 2015 to close out, and if necessary, to refund any unused monies in the Energy Storage Balancing Account."
- Action Performed: On June 24, 2013, SDG&E submitted advice letter 2495-E. On page 2 of that AL, SDG&E asked to establish the ESBA per the rules in D.13-05-010. The ESBA was set up as a one-way balancing account to capture the revenue requirement and actual costs associated with the $26 million capital funding authorized. On July 23, 2013, SDG&E was notified by Energy Division that that AL had been suspended. On November 25, 2013, AL 2495-E was approved and made effective July 24, 2013.
  - The ESBA is still in effect. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the ESBA.
- Status: Completed.

6. <u>Transmission Integrity Management Program Balancing Account ("TIMPBA").</u>

- Source: TY2012 GRC Decision, OP 16; Findings of Fact 183; and Page 387.
- Requirement: "SDG&E is authorized to establish a two-way balancing account to recover the operations and maintenance costs, and capital expenditures costs, of complying with the transmission integrity management program. SDG&E shall file a Tier 2 Advice Letter within 45 days of the effective date of this decision to establish this balancing account."
- Action Performed: On June 24, 2013, SDG&E submitted advice letter 2495-E. On page 2 of that AL, SDG&E asked to establish the TIMPBA per the rules in D.13-05-010. The TIMPBA was set up as a two-way balancing account to capture the record the difference between the authorized revenue requirement and actual costs associated with SDG&E's TIMP for the 2012 test year GRC cycle. On July 23, 2013, SDG&E was notified by Energy Division that that AL had been suspended. On November 25, 2013, AL 2495-E was approved and made effective July 24, 2013.
  - The TIMPBA is still in effect. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the TIMPBA.
- Status: Completed.

7. Post-2011 Distribution Integrity Management Program Balancing Account ("Post-2011 DIMPBA").

- Source: TY2012 GRC Decision, OP 17; and Pages 392-393.
- Requirement: "SDG&E is authorized to establish a two-way balancing account to recover the operations and maintenance costs, and capital expenditures costs, of complying with the distribution integrity management program. SDG&E shall file a Tier 2 Advice Letter within 45 days of the effective date of this decision to establish this balancing account and to close out its current distribution integrity management program balancing account (DIMPBA). Any balance remaining in the DIMPBA shall be amortized in gas transportation customers' rates."
- Action Performed: On June 24, 2013, SDG&E submitted advice letter 2495-E / 2204-G. On page 2 of that AL, SDG&E asked to establish the Post-2011 DIMPBA per the rules in D.13-05-010. The Post-2011 DIMPBA was set up as a two-way balancing account to capture the record the difference between the authorized revenue requirement and actual costs associated with SDG&E's DIMP for the 2012 test year GRC cycle. On July 23, 2013, SDG&E was notified by Energy Division that that AL had been suspended. On November 25, 2013, AL 2495-E-A / 2204-G-A was approved and made effective July 24, 2013.
  - On Page 3 of the same AL 2495-E-A / 2204-G-A, SDG&E asked to close out the existing DIMPBA. That request was approved in AL 2204-G-A
  - The Post-2011 DIMPBA is still in effect. Please refer to the Direct Testimony of Norma Jasso (Ex. SDG&E-35) for a discussion of the Post-2011 DIMPBA.
- Status: Completed.

8. Refund the balances in various Regulatory Accounts, as part of SDG&E's request in the 2012 GRC.

- Source: TY2012 GRC Decision, Page 974.
- Requirement: SDG&E is required to amortize the balances in the respective Regulatory Accounts. These amounts in the 2012 GRC were revised amounts from Exhibits 262 and 264 and updated in Exhibit 596.
- Action Performed: In reference to the Advanced Metering Infrastructure Balancing Account ("AMIBA"), paragraph 4 on page 974 of D.13-05-010 points to Exhibit 596 and says "there is an overcollection of $11.041 million on the electric side, and an undercollection of $3.830 million on the gas side." The decision then grants SDG&E's request to dispose of those balances. By the time a decision was reached on the 2012 GRC, those balances were different than forecasted back during the application. In fact, on September 9, 2010, SDG&E filed a Petition for Modification

("PFM") requesting the Commission modify D.07-04-043 to clarify the accounting rules to extend the balancing account until such time as the project was complete and a final reconciliation of the account could be performed. That PFM was approved in D.11-03-042 on March 24, 2011. As such, the balances that remain in the AMIBA are being retained until such time as the account can be finalized with the conclusion of the project. Therefore, the incorporation of these AMIBA balances is still in progress. Further, in the 2012 GRC application (A.10-12-050) my Direct Testimony on the topic of Regulatory Accounts (Exhibit SDGE-41) I discussed the AMIBA balance. On Page GDS-4 of that exhibit, I proposed that "any remaining balance in the AMI electric and gas balancing accounts at the end of the GRC cycle, as well as the final calculation of the sharing mechanism associated with the project, will be addressed in the next GRC." Please see the Direct Testimony of Norma Jasso (Ex. SDG&E-35) in this immediate application for SDG&E's proposal to transfer any AMIBA balances to the appropriate Fixed Cost Accounts.

- Another account discussed for disposition on Page 974 of D.13-05-010 is the DIMPBA. As discussed above in this testimony, the DIMPBA was disposed of in AL 2204-G-A. The balance in the DIMPBA at the time D.13-05-010 was issued was no longer the overcollection of $70,084 referenced in D.13-05-010 on page 974. The balance had turned undercollected and because the account was a one-way account, the balance was not put into rates. Therefore the incorporation of the DIMPBA balance is complete.
- Lastly, Page 974 of D.13-05-010 calls for the balance in the Research, Development & Demonstration Expense Account ("RDDEA") of $46.379 to be amortized in rates. That balance was put into rates on September 1, 2013, in accordance with AL 2485-E-A. Therefore the incorporation of the RDDEA balance into rates is complete.

- Status: While the treatment of the balance in the AMIBA is pending this application, the incorporation of the DIMPBA and the RDDEA is complete.

E. Other Topics

1. Provide a showing on the derivation and justification of Allowance for Funds Used During Construction ("AFUDC") rates.

   - Source: TY2012 GRC Decision, OP 28; Conclusion of Law 64; and Page 991.
   - Requirement: "San Diego Gas & Electric Company shall provide in its next general rate care application a detailed showing on the derivation of and justification for their respective proposed Allowance for Funds Used During Construction (AFUDC) rates…and shall include at least the following: a.) recorded and forecast AFUDC rates, determined consistent with the FERC rule and formula, for each year between 2012 and the 2016 test year. Supporting documentation shall include each component of the FERC formula. b) The amount and average cost of short-term debt carried or forecast to be carried yearly during the 2012 through 2016 period. c.) The purposes for which short-term debt was used or is forecast to be used, and the amounts of short-term debt for each purpose, yearly during the 2012 through 2016 period."
   - Action Performed: Please refer to the Direct Testimony of SDG&E witness Jesse Aragon (Ex. SDG&E-27) for this showing and the derivation of SDG&E's AFUDC.
   - Status: Completed.

2. Ending the Sustainable Community energy system project at the end of the GRC cycle.

   - Source: TY2012 GRC Decision, OP 8; Finding of Fact 57; and Page 181.
   - Requirement: "The sustainable community energy system project for San Diego Gas & Electric (SDG&E) shall end at the end of the General Rate Case (GRC) cycle."
   - Action Performed: SDG&E is winding down the Sustainable Community Energy project. As addressed in the Direct Testimony of John Jenkins (Ex. SDG&E-09), SDG&E is asking for no funding for this project in the 2016 estimate.
   - Status: Completed.

3. Reliability Performance Incentives.

   - Source: TY2012 GRC Decision, OP 9; Finding of Fact 65; Conclusions of Law 14, 15, 16; and Page 107.
   - Requirement: "San Diego Gas & Electric Company is directed to file a Tier 3 advice letter within 90 days of the effective date of this decision, proposing a set of reliability performance incentives consistent with what was adopted in D.08-07-046, updating the targets that would have been in

effect in 2010. The advice letter shall include at a minimum the system average interruption duration index (SAIDI), system average interruption duration exceeding threshold (SAIDET), and system average interruption frequency index (SAIFI) with proposed targets, dead bands, increments, rewards, penalties and maximum amounts, and annual improvement measures for each index."

- Action Performed: On September 6, 2013, SDG&E filed AL 2518-E, "Proposed Reliability Performance Incentives in Compliance with CPUC Decision 13-05-010 Ordering Paragraph 9." The purpose of that AL was to comply with the direction that SDG&E propose a set of reliability performance incentives consistent with those set in D.08-07-046. That AL also serves the purpose of proposing an alternative set of reliability performance incentives.
  - Prior to that AL, SDG&E had filed a request for additional time to comply with OP 9 of D.13-05-010 in order to continue discussion with the Coalition of California Utility Employees ("CCUE").
  - Since the filing of the AL, suspension letters have been sent to SDG&E, the most recent on January 4, 2014. SDG&E filed a petition to modify D.13-05-010 on March 17, 2014 for the purpose of proposing an alternative performance-based ratemaking ("PBR") mechanism that is consistent with the intent of OP 9, while taking into account the excellent state of electric reliability at SDG&E. On September 11, 2014 the petition to modify was approved (D.14-09-005).
  - On June 18, 2014, SDG&E received a letter from Edward Randolph, Director Energy Division, rejecting AL 25-18-E without prejudice. In that letter, the Energy Division states that SDG&E is in compliance with D.13-05-010 in its filing of AL 2518-E:

    > "SDG&E complied with OP 9 of D. 13-05-010 by filing AL 2518-E. SDG&E also made clear in AL 2518-E that its preference would be to move to an alternative set of reliability performance incentives that it claims would enable it to better focus on reliability improvements in areas where improvements are most needed. Since SDG&E's PFM (March 17, 2014), is now the Commission's procedural venue for deciding this matter, AL 2518-E is rejected without prejudice at this time."

- Status: Completed (in compliance with OP 9).

4. <u>Inclusion of a discussion of reliability measures.</u>

- Source: TY2012 GRC Decision, Page 208.
- Requirement: "In its next GRC filing, SDG&E must include a discussion and a summary of the reliability measures, with a comparison to the data

from 2 prior GRC cycles and also a summary of cause of outages and trends."

- Action Performed: Please see the Direct Testimony of Jonathan Woldemariam (Ex. SDG&E-10) for this discussion and summary.
- Status: Completed.

5. Developing a public education program involving pipeline excavations and identifying gas leaks.

- Source: TY2012 GRC Decision, Page 394.
- Requirement: "Under 49CFR section 192.616, SDG&E must develop and implement a public education program to educate the public, government organizations, and persons engaged in excavation about procedures to follow involving pipeline excavations and how to identify gas leaks. That regulation also requires SDG&E to notify municipalities, school districts, businesses, and residents of pipeline locations."
- Action Performed: SDG&E has developed and implemented a federally-mandated Public Awareness program, as prescribed in 49 CFR 192.616. The Public Awareness program principally seeks to educate the public to understand the following:
  - How to recognize a natural gas leak;
  - How to properly respond in the event of gas leak, and;
  - How to help prevent personal injury or property damage.
  - Additional information on this for the TY2016 GRC is found in the testimony of witness Raymond Stanford (Ex. SDG&E-06).
- Status: Completed.

6. Accounting for prefunded postage.

- Source: TY2012 GRC Decision, Conclusion of Law 34.
- Requirement: "Prefunded Postage must be accounted for by SDG&E in FERC Account #165, instead of being included as part of postage expense."
- Action Performed: Beginning on June 1, 2012, SDG&E began using the pre-paid asset account 165 to record the deposits made with the United States Postal Service in compliance with the Conclusion of Law #34. Postage is only recorded as an O&M expense when the actual expenses are incurred. Please reference the Direct Testimony of Bradley Baugh (Ex. SDG&E-14) for more information.
- Status: Completed.

7. SDG&E to conduct independent audit of data privacy and security practices.

- Source: TY2012 GRC Decision, OP 4.
- Requirement: "SDG&E will conduct independent audits of its electricity usage data privacy and security practices in conjunction with General Rate Case (GRC) proceedings following 2012 and at other times as required by order of the Commission. Pursuant to OP 3 of D.12-08-045, SDG&E will conduct independent audits of its gas usage data privacy and security practices. The audits will monitor compliance with data privacy and security practices described in D. 11-07-056 and D. 12-08-045, and SDG&E will report the findings to the Commission as part of its GRC filing."
- Action Performed: In April 2014, SDG&E contacted the outside independent consulting firm of KPMG to conduct the audit in compliance with OP 4. The audit was mobilized in May 2014. The completed Audit Report can be found in Appendix A of this exhibit.
- Status: Complete.

8. Convene the Energy Efficiency Finance Programs Data Working Group to finalize EE finance program reports.

- Source: D. 13-09-044, OP 13.
- Requirement: D.13-09-044 directed the IOUs to convene the Energy Efficiency (EE) Finance Programs DWG to finalize its March 2012 draft report which identifies data collection requirements for all post-2012 EE finance programs, and associated activities and documents (e.g., customer consent forms).
- Action Performed: In compliance with D. 13-09-044, a public workshop was conducted on November 13, 2013, covering the draft report and other significant considerations regarding the collection of data to support deployment and ongoing implementation of the pilots. On December 16, 2013, the Southern California Gas Company filed AL 2557-E/2252-G on behalf of itself, SDG&E, and two other California utilizes. Attachment B of that AL includes the final report of the Data Working Group. On February 7, 2014, AL 2557-E/2252-G was approved effective December 16, 2013.
- Status: Completed.

9. Submit annual Electric Program Investment Charge.

- Source: D. 12-05-037, OP 16; and D.13-11-025, Attachment 5.
- Requirement: SDG&E and its fellow EPIC Administrators are required to each submit an annual report "detailing program activities." The annual reports are designed "to facilitate consistent reporting by the [EPIC] Administrators on their investment plans and project results." The reports, and their timing, are intended to inform stakeholders of the EPIC Plan's

accomplishments when they meet with the EPIC administrators in March of the years in which investment plans will be considered.

- Action Performed: SDG&E submitted its 2013 EPIC Annual Report on February 28, 2014. This Report provides an overview of SDG&E's EPIC activities up to and during the 2013 calendar year. This Report also includes information on SDG&E's Plug-in Electric Vehicle submetering pilot program activities up to and during the 2013 calendar year because SDG&E intends to fund the PEV submetering pilot program with EPIC funds. Additional information about SDG&E's EPIC and PEV submetering pilot program activities can be found in Attachment B, referred to as "SDG&E 2013 EPIC Project Status Report," of that filed 2013 EPIC Annual Report.
- Status: Completed.

10. Social Media and internet-related function available to SDG&E customers.

- Source: D. 13-05-010, Page 473.
- Requirement: "SDG&E is directed to provide in its next GRC filing a description of all of its internet-related and social media functions that are available to its customers or that it is planning, the reasons for providing those functions and their cost effectiveness, and how the call centers have been or will be integrated or utilized to provide those functions."
- Action Performed: Appendix A of the Direct Testimony of Brad Baugh (Ex. SDG&E-14) contains the descriptions and summaries of the benefits relating to social media as they relate to SDG&E's Customer Contact Centers.
- Status: Completed.

III. CONCLUSION

This concludes my prepared direct testimony.

IV. WITNESS QUALIFICATIONS

My name is Gregory D. Shimansky. My business address is 8330 Century Park Court, San Diego, California 92123. I am employed by SDG&E as the GRC Program Manager for both SDG&E and SoCalGas. I have held this position since June of 2013. Prior to this position I was the Regulatory Accounts and Financial Services Manager at SDG&E in the Financial Analysis Department for 3 years. In that position, I was responsible for managing the process for the development, implementation, and analysis of regulatory balancing and memorandum accounts as well as supervising the treasury function at SDG&E.

I have been employed with SDG&E, SoCalGas and Sempra Energy since June 30, 2003. In addition to my current position in the GRC organization, I served as the Financial Planning Manager for Sempra Energy, the Regulatory Reporting Manager at SDG&E/SoCalGas, and from June 2003 through August 2008, I worked for SDG&E in utility planning. I earned a Bachelor of Science degree in Economics from the University of California, Los Angeles in June 1993. I also earned a Master of Science in Management, with concentrations in Finance and Marketing, from Purdue University in May 1998.

I have previously provided testimony to the Commission.

Appendix A

CPUC Covered Information Privacy and Security Assessment Report

KPMG

cutting through complexity

San Diego Gas & Electric

CPUC Covered Information Privacy and Security Assessment Report

September 15, 2014

Table of Contents

Document Structure

This report consists of the following sections:

Executive Summary contains an overview of the project including background, scope, and KPMG's overall conclusion and noted exceptions and recommendations for each Rule comprising the *California Public Utility Commission (CPUC) Privacy Decisions*.

Project Approach and Methodology contains an overview of key project phases and activities performed by KPMG throughout the course of the assessment.

Rule Conclusions, Exceptions and Recommendations provides a summary of the nine (9) Rules of the *CPUC Privacy Decisions* issued on July 29, 2011 and August 23, 2012 including KPMG's interviews and document reviews (e.g., test work), conclusions, detailed exceptions, and improvement recommendations associated with each Exception.

San Diego Gas & Electric's Management Response to CPUC Covered Information Privacy and Security Assessment Report contains SDG&E's Management response to the *CPUC Covered Information Privacy and Security Assessment Report* dated September 15, 2014.

Appendix: Detailed Test Procedures and Results provide the full details of KPMG's assessment criteria procedures and results for each Rule.

Executive Summary

San Diego Gas & Electric (SDG&E) provides energy service to 3.4 million people through 1.4 million electric meters and 860,000 natural gas meters in San Diego and southern Orange County. Through its operations, SDG&E collects, processes, stores, and discloses Customer Energy Usage Data (CEUD) and other Customer Personally Identifiable Information (PII). The PII may contain name, address, social security numbers (SSN), service account numbers, and financial account information.

Background

On July 29, 2011, the California Public Utilities Commission (CPUC) issued Decision D.11-07-056 *Rules Regarding Privacy and Security Protections for Energy Usage Data*. In addition, the CPUC issued a second decision D.12-08-045 *Decision Extending Privacy Protections to Customers of Gas Corporations and Community Choice Aggregators and to Residential and Small Commercial Customers of Electric Service Providers* on August 23, 2012, (the "*Privacy Decisions*"). The *Privacy Decisions* require San Diego Gas & Electric (SDG&E) to undergo an independent assessment of its "Covered Information" privacy and security practices. Covered Information is defined in the *Privacy Decisions* as Customer Energy Usage Data (Covered Information) obtained via Advanced Metering Infrastructure (AMI) combined with other Customer PII that could reasonably be used to identify a residential customer, family, household, residence, or nonresidential customer.

SDG&E engaged KPMG to conduct an independent assessment of its Covered Information privacy and security controls and this report represents the results of the KPMG assessment of SDG&E's privacy and security practices.

Scope

The scope of KPMG's assessment was Covered Information and review was limited to systems and organizational units (OUs) collecting, processing, storing, or disclosing Covered Information. The scope did not cover SDG&E's employee, contractor, and other PII other than Covered Information.

To perform the review, KPMG developed an Assessment Framework comprised of multiple criteria based on various industry leading standards. We mapped the Assessment Framework criteria to the nine (9) Rules in the *Privacy Decisions* and used the Framework to perform our assessment of SDG&E's practices and procedures.

- The Exceptions and Recommendations were based on review of policy/procedure documents, stakeholder interviews, inspection of samples and systems, and site walkthroughs.
- KPMG conducted interviews with personnel from Customer Services, (includes Customer Programs, Office of Customer Privacy (OCP), Customer Billing Operations, Credit Operations, Customer Pricing), Residential Services, Smart Meter Operations, Customer Call Centers (CCC), Branch Office, Information Security (IS) & Information Management, Computing Infrastructure, Legal, Governance and Compliance, Financial Systems & Compliance, Direct Access, Audit Services, Human Resources (HR) – Training, Support Services, Remittance Processing, Supplier Management, Energy Markets & Capacity Products, SDG&E Application Services, Regulatory Affairs, and Business Controls and Compliance.
- KPMG performed a test of design and implementation of privacy and security controls followed by test work of the operating effectiveness of the key implemented controls.

- The Covered Information Privacy and Security Practices Assessment was based on KPMG's review and understanding of the controls and processes during the Period of Review from **April 1, 2013 to March 31, 2014.**[1]

The nine (9) Rules noted in the *Privacy Decisions* are listed below.

Rule 1	Definitions
Rule 2	Transparency (Notice)
Rule 3	Purpose Specification
Rule 4	Individual Participation (Access and Choice)
Rule 5	Data Minimization
Rule 6	Use and Disclosure Limitation
Rule 7	Data Quality and Integrity
Rule 8	Data Security
Rule 9	Accountability and Auditing

Overall Conclusion

KPMG has noted **4** Exceptions (Exceptions are areas where SDG&E's program is not yet fully prepared to meet compliance with the *Privacy Decision*). The Exceptions are shown below along with the Recommendations associated with each Exception. There were **no** High-Risk Exceptions; **3** Medium-Risk Exceptions, and **1** Low-Risk Exceptions.[2]

[1] KPMG used the following key drivers to determine the audit period: (1) The *CPUC Privacy Decision* does not define the audit period; (2) The majority of SDG&E's privacy and security controls became effective after April 1 2013; and (3) Professional guidance for initial assessments provides flexibility in the period covered as long as the audit period allows for sufficient time to test Operating Effectiveness.

[2] See "Rule Conclusions, Exceptions and Recommendations" section on Page 9 for Exception Severity definitions.

CPUC Rule Number	Risk Level	Exceptions Noted	KPMG Recommendations
CPUC Rule 1 Definitions	-	-	N/A
CPUC Rule 2 Transparency (Notice)	-	-	N/A
CPUC Rule 3 Purpose Specification	-	-	N/A
CPUC Rule 4 Individual Participation (Access and Choice)	-	-	N/A
CPUC Rule 5 Data Minimization	-	-	N/A
CPUC Rule 6 Use and Disclosure Limitation	**Medium**	New vendor contracts contain provisions requiring Third Parties to agree to safeguard Covered Information under policies, practices, and notification requirements no less protective than those under which SDG&E operates. However, some existing, active vendor contracts may require a lower standard of safeguarding Covered Information consistent with the policies, practices, and notification requirements of the Third Party.	SDG&E should assess whether previously executed Third Party contracts contain provisions to sufficiently safeguard Covered Information. SDG&E should work with the contracting party to amend existing contract language to require Third Parties to agree to safeguard Covered Information under policies, practices and notification requirements no less protective than those under which SDG&E operates.
CPUC Rule 7 Data Quality and Integrity	-	-	N/A
CPUC Rule 8 Data Security	**Medium**	No formal standards or procedures have been published to inform employees of requirements to protect data based on its classification.	Management should update the existing *Data Classification Guidelines* to identify the required logical, physical, and administrative security controls to be applied to information or systems containing information that are classified as "Confidential" or "Restricted".

CPUC Rule Number	Risk Level	Exceptions Noted	KPMG Recommendations
	Medium	The password configuration of a Third Party-hosted application, which stores commercial customer usage data, is not in line with the Sempra Password Standard. The application does not currently enforce password complexity requirements (e.g., minimum length, alphanumeric and special characters). In addition, the application team does not apply password complexity standards when creating master user account initially or when assigning an initial password to customer accounts. SDG&E is currently working with the application vendor to update the application password configuration to be in line with the Sempra Password Standard requirements.	SDG&E should enforce stronger password practices by creating an account password that complies with Sempra Password Standard upon creation of the user account. In addition, SDG&E should consult with the application vendor to update the application password parameters to be aligned with the Sempra Password Standard.
CPUC Rule 9 Accountability and Auditing	**Low**	While company-wide Customer Privacy training was developed it was not consistently rolled out to cover new employees hired after the training was initially launched, or certain contractors with access with Covered Information.	SDG&E should implement a standardized training requirement addressing the safeguarding of Covered Information for contractors hired through a temporary work-force solution that have access to Covered Information.

Project Approach and Methodology

KPMG approached the Assessment in five (5) phases: Mobilize, Discover, Assess, Validate, and Report.

- **Mobilize –** KPMG developed an Assessment Framework to review SDG&E's privacy and security practices on the nine (9) Rules comprising the *Privacy Decisions*. We identified controls for each Rule's requirements and performed procedures to test the Design and Implementation and Operating Effectiveness of program policies and procedures to identify any noted exceptions to those controls. Given the similarity of the Generally Accepted Privacy Principles (GAPP) framework promulgated by the American Institute of Certified Public Accountants (AICPA) and CPA Canada, we leveraged GAPP as a baseline to develop our testing procedures.
- **Discover –** KPMG worked with the SDG&E Privacy Project Team to identify relevant stakeholders, reviewed the organizational structure to identify business groups where Covered Information may reside, and reviewed the current IT landscape to identify systems and applications that collect, store, or process Covered Information, such as Advanced Meter Systems, Customer Information Systems applications and databases, Back-end systems, Middleware, Development/Test environments, and Customer Portals.
- **Assess –** As part of our, KPMG performed a variety of interviews with stakeholders representing Executive Leadership, Corporate Shared Services departments, and SDG&E. A total number of 70 personnel were interviewed; more than 250 documents reviewed; and we performed five (5) site walkthroughs of critical SDG&E facilities (including the Customer Contact Center, a Production and Backup Datacenter, Credit & Collections and Billing Operations, Branch Office, and the Bill Print and Remittance Processing Center) to observe the safeguards in place to protect Covered Information.
- **Validate –** KPMG validated all observed Exceptions throughout the Assessment phases with the SDG&E Privacy Project Team, relevant business and IT stakeholders, and leadership.
- **Report –** KPMG developed a final report providing Exceptions and Conclusions, presented the report to SDG&E Leadership, and incorporated Management Response to the noted Exceptions.

Rule Conclusions, Exceptions and Recommendations

KPMG notes **4** specific Exceptions, which are areas where SDG&E's program is not yet fully prepared to meet requirements under the *Privacy Decisions*. For any risk identified, KPMG reviewed the risk and assigned a risk rating of **High, Medium,** or **Low** to each Exception based on the potential impact the Exception could have as it relates to the protection of Covered Information. The risk rating methodology is based on KPMG's experience as well as industry leading practices and standards

There were **no** High-Risk Exceptions**; 3** Medium-Risk Exceptions, and **1** Low-Risk Exception.

Risk Level	Description
High	Issue poses a significant risk of data breach of Covered Information and/or a significant deviation from the *CPUC Privacy Decisions*.
Medium	Inconsistent implementation of policies and procedures that may impact the ability of SDG&E to protect Covered Information and/or achieve adequate alignment with the *CPUC Privacy Decisions*.
Low	Undefined or undocumented policies and procedures supporting the protection of Covered Information and alignment with the *CPUC Privacy Decisions.*

The following tables provide a summary of the criteria that KPMG applied in the testing of each of the nine (9) Rules of the *Privacy Decisions*, the overall conclusion of the set of criteria evaluated, relevant Exceptions (if any) along with level of risk, risk implication and Recommendation.

Rule 2: Transparency

KPMG Testing Summary	KPMG performed testing of SDG&E's overall customer notice program focusing on: ■ Internal and customer-facing *Privacy Policies* and *Notices* that address SDG&E's practices and procedures related to the collection, processing, storage, and disclosure of their Covered Information; ■ Review of methods and frequency for providing customers with notice and an examination of the actual notices; ■ Interviews with SDG&E personnel; ■ Performance of site walkthroughs of Customer Service facilities to observe Energy Service Specialists interacting with customers and discussing their Covered Information.
KPMG Test Results Summary	KPMG determined that SDG&E provides its external-facing *Privacy Policy* and *Privacy Notice* on its website detailing the manner in which the company collects, stores, shares, and protects Covered Information and the methods by which customers can access their data. The *Privacy Notice* includes information on how customers can contact SDG&E with complaints, inquiries, and disputes. SDG&E also provides its *Privacy Notice* to newly registered customers as part of a welcome package, and annually thereafter in a bill statement.
Exception	No Exceptions Noted
Risk Level	-
Risk Implication	-
Recommendation	-

Rule 3: Purpose Specification

KPMG Testing Summary	KPMG performed testing of SDG&E's specification of the purposes focusing on: ■ How SDG&E specifies the reasons for which it collects, discloses, retains, and provides access to Covered Information; ■ Review of the SDG&E *Privacy Notice* and other policies and procedures and interviews with stakeholders to understand the determination and specification of information and Third Party categories; ■ Examination of whether the *Privacy Notice* included a description of how customers could access and control their Covered Information collected, processed, stored, and disclosed by SDG&E.
KPMG Test Results Summary	KPMG found that SDG&E has documented policies and procedures outlining the acceptable purposes for which Covered Information may be collected, stored, and shared, including detailed policies regarding Primary and Secondary Purposes. The SDG&E *Privacy Notice* includes the categories of Third Parties with which SDG&E shares Covered Information. SDG&E has implemented internal policies instructing employees on determining the veracity and propriety of Third Party requests, and on the appropriate use of Covered Information internally.
Exception	No Exceptions Noted
Risk Level	-
Risk Implication	-
Recommendation	-

Rule 4: Individual Participation (Access and Choice)

KPMG Testing Summary	KPMG performed testing of SDG&E's customer-facing program focusing on: ■ Internal and external policies and procedures to provide customers with access and consent mechanisms related to their Covered Information; ■ Review of Customer Portals, stakeholder interviews conducted, and performance of walkthroughs of the Contact Center and Branch Office locations where SDG&E Energy Service Specialists (ESS) interact with customers with respect to their Covered Information; ■ Review of Customer Authorization forms to understand how customers can grant and revoke authorization for secondary uses of their Covered Information; ■ Examination of the process in place to disclose Covered Information pursuant to legal processes and in situations of imminent threat to life or property. Test procedures included review of policies and procedures for tracking these requests and the subsequent notice provided to customers and interviews with SDG&E stakeholders in relevant business functions.
KPMG Test Results Summary	KPMG determined that SDG&E provides customers with multiple methods to access their Covered Information, including via the My Account and kWickview features online and home energy reports which allow them to review and interpret their online usage information. SDG&E has implemented the Green Button initiative allowing customers to download up to 13 months of their Covered Information and connect that data with Third Parties for analysis. Further, internal guidelines for SDG&E employees who interact with customers are in place addressing how to allow customers access to their Covered information. Customers may also visit one of SDG&E's five Branch Offices to make payments, perform service requests, or receive a copy of their bill including usage data. SDG&E has processes and procedures in place for customers to grant and revoke authorization to Third Parties for Secondary Purposes of Covered Information through the use of a Customer Information Service Request (CISR) form. Customer facing policies and notices indicate SDG&E may disclose Covered Information if it is necessary to comply with relevant laws, to respond to subpoenas or warrants, or to emergency responders in the case of imminent threat to life or property in which case customers would be notified.
Exception	No Exceptions Noted
Risk Level	-
Risk Implication	-
Recommendation	-

Rule 5: Data Minimization

KPMG Testing Summary	KPMG performed testing of SDG&E's adoption of Data Minimization principles in the collection, use, and disclosure of Covered Information focusing on: ■ Review of corporate and department-specific policies and procedures to understand how Covered Information is segregated from other systems; ■ How user access is restricted based on business need; ■ How records and assets are retained for only for as long as reasonably necessary; ■ Proper disposal of records upon their eligibility for destruction; ■ Examination of how Data Minimization principles were adopted as part of Third Party disclosure practices. Test procedures included review of policies and procedures and interviews with relevant stakeholders to understand appropriate safeguards in place to limit the disclosure of Covered Information.
KPMG Test Results Summary	KPMG determined that SDG&E has implemented the Data Minimization principle as a foundational component to its overall privacy framework, and has documented policies and procedures limiting the amount of information collected, stored and retained, and the data elements and categories of Third Parties with whom it is shared. SDG&E management reviews and certifies that Covered Information is retained as necessary, and that it is properly disposed of in electronic, hardcopy, and unstructured formats in a timely manner.
Exception	No Exceptions Noted
Risk Level	-
Risk Implication	-
Recommendation	-

Rule 6: Use and Disclosure Limitation

KPMG Testing Summary	KPMG performed testing of SDG&E's Third-Party Management Program focusing on: ■ Review of processes in place for disclosure of Covered Information to Third Parties; ■ Review of procedures and forms for customers to authorize and revoke a Third Party to receive Covered Information on behalf of the customer; ■ Examination of Third-Party management policies and procedures and interview stakeholders to understand how SDG&E implements practices and procedures based on the categories of Third Parties (i.e., Primary Purpose and Secondary Purpose); ■ Review of data transmission protocols and ongoing monitoring of Third Parties for compliance with SDG&E and Supply Management (Corporate Shared Services department) policies and contractual provisions.
KPMG Test Results Summary	KPMG found that SDG&E has processes in place to allow customers to share their Covered Information data with Third Parties. SDG&E has internal formal procedures to manage customer requests of disclosure to Third Parties which include forms for explicit customer authorization and forms to revoke such authorization (CISR forms). SDG&E has internal Third-Party management policies and informs suppliers and Third Parties about data privacy requirements. Third Party vendors are contractually obligated per their contract clauses to maintain the privacy of the information shared.
Exception	New vendor contracts contain provisions requiring Third Parties to agree to safeguard Covered Information under policies, practices, and notification requirements no less protective than those under which SDG&E operates. However, some existing, active vendor contracts may require a lower standard of safeguarding Covered Information consistent with the policies, practices, and notification requirements of the Third Party.
Risk Level	Medium
Risk Implication	Third Party data security practices may not be sufficient to safeguard Covered Information heightening SDG&E's legal and regulatory exposure and increasing the risk of a potential breach of customer data.
Recommendation	SDG&E should assess whether previously executed Third Party contracts contain provisions to sufficiently safeguard Covered Information. SDG&E should work with the contracting party to amend existing contract language to require Third Parties to agree to safeguard Covered Information under policies, practices and notification requirements no less protective than those under which SDG&E operates.

Rule 7: Data Quality and Integrity

KPMG Testing Summary	KPMG performed testing of SDG&E's Data Validation methods and procedures focusing on: ■ Review of how SDG&E validates the quality and integrity of Covered Information; ■ Examination of the Smart Meter systems and infrastructure to understand how usage data is managed and reconciled; ■ Review of policies and procedures and interviewed stakeholders to understand how SDG&E provides customers with the opportunity to modify or remove other data elements collected by the company.
KPMG Test Results Summary	KPMG found that SDG&E has policies in place that address the confirmation, validation, and relevance of customer information. It is clearly stated within the *Privacy Notice* that customers may contact SDG&E should they need to update or make any alterations to their information. In addition, call center personnel authenticate customers and validate their account information when answering a call. When accessing their online account, customers are notified that it is the responsibility of the customer to ensure their personal information is updated and accurate. KPMG found that meter data consumption and processing systems validate Energy Usage reads and perform edits to ensure completeness and accuracy of usage data prior to billing the customer.
Exception	No Exceptions Noted
Risk Level	-
Risk Implication	-
Recommendation	-

Rule 8: Data Security

KPMG Testing Summary	KPMG performed testing of SDG&E's physical and Cyber security measures to protect Covered Information focusing on: ■ Review of Information Security (Corporate Shared Services department) policies, procedures and measures related to: Endpoint Security (Antivirus protection, E-mail/Database security), the Network environment (Network Segmentation, Intrusion Detection/Prevention Systems, Remote Access, Wireless) Firewalls, Network Access Control, (Logging/Monitoring, Data Loss Prevention, Web-content Filtering), Mobile Security, Patch Management, Vulnerability Management, Business Continuity, Change Control, Privileged Access, Third Party Access and Data Classification; ■ Performance of site walkthroughs at critical SDG&E locations focusing on the physical and technical security of Covered Information at these key areas: Customer Contact Center, Branch Office, production and backup Data Centers, Bill Print and Remittance Processing, and Credit Operations; ■ Inspection of key configurations and system settings related to: System Access (User Authentication and Password Configuration), Access Management (Restriction of access based on least privilege and need-to-know, Segregation of Duties, Periodic review of access), Logging and Monitoring of changes to customer data, Masking of sensitive data in production and development environments; ■ Inspection of key configurations and system settings related to: System Access (User Authentication and Password Configuration), Access Management (Restriction of Access based on least privilege and need-to-know, Segregation of Duties, Periodic review of access), Logging and Monitoring of changes to customer data, Masking of sensitive data in production and development environments; ■ Review of SDG&E/Corporate Shared Services department's Incident Response/Breach Management Program and interviews with stakeholders who are responsible and/or accountable in the response to a potential incident involving Covered Information including communications to regulators and impacted customers; ■ Examination of evidence of tools deployed in the environment to detect and analyze potential threats to Covered Information.
KPMG Test Results Summary	KPMG found that SDG&E has appropriate policies, procedures and measures for the following areas: Endpoint Security, Network environment, Firewalls, Mobile Security, Patch Management, Vulnerability Management, Business Continuity, Change Control, Privileged Access, and Third Party Access. Additionally, KPMG found that SDG&E currently has in place physical security controls to limit the risk of unauthorized access to Covered Information at critical facilities. Furthermore, SDG&E has a mature Incident Response/Breach Management Program consisting of documented policies and procedures. The Incident Response Process is owned by Information Security (Corporate Shared Services department) and different Business Units throughout the enterprise (including Legal and the SDG&E Office of Customer Privacy) that have responsibilities in response to a potential data incident. Training is provided to employees through Awareness Campaigns. We noted that SDG&E performs ongoing testing of its plan through IT incident logging and PII Tabletop Drills/Exercises involving representation from critical business units that collect, handle, store, and disclose Covered Information.
Exception 1	No formal standards or procedures have been published to inform employees of requirements to protect data based on its classification.

Risk Level	Medium
Risk Implication	More sensitive data classes may be collected, used, processed, or disposed of at a standard that does not adequately safeguard the data.
Recommendation	Management should update the existing *Data Classification Guidelines* to identify the required logical, physical, and administrative security controls to be applied to information or systems containing information that are classified as "Confidential" or "Restricted".
Exception 2	The password configuration of a Third Party-hosted application, which stores commercial customer usage data, is not in line with the Sempra Password Standard. The application does not currently enforce password complexity requirements (e.g., minimum length, alphanumeric and special characters). In addition, the application team does not apply password complexity standards when creating master user accounts initially or when assigning an initial password to customer accounts. SDG&E is currently working with the application vendor to update the application password configuration to be in line with the Sempra Password Standard requirements.
Risk level	Medium
Risk Implication	Malicious users may have easier access to SDG&E corporate customer Covered Information by guessing the customer's application password.
Recommendation	SDG&E should enforce stronger password practices by creating an account password that complies with Sempra Password Standard upon creation of the user account. In addition, SDG&E should consult with the application vendor to update the application password parameters to be aligned with the Sempra Password Standard.

Rule 9: Accountability and Auditing

KPMG Testing Summary	KPMG performed testing of SDG&E's overall Customer Data Privacy and Cybersecurity program, focusing on: ■ Review of documentation supporting each program as well as SDG&E's communication of these policies to both employees and contractors; ■ Review of executive support and sponsorship of Customer Data Privacy and Cybersecurity including the individuals and roles responsible and accountable for Customer Data Privacy and Cybersecurity throughout the enterprise; ■ Interviews with members of Sempra and SDG&E Executive Management to understand the tone at the top as well as leadership's views on customer data protection; ■ Review of the process to receive, track and resolve customer complaints, disputes, and inquires related to the protection of their Covered Information. Test procedures included a review of internal procedures, interviews with stakeholders involved in the Complaints Process, and a walkthrough of the Customer Contact Center; ■ Examination of employee training and awareness programs associated with the protection of Covered Information. This testing included a review of enterprise-wide and targeted training materials provided to business units and Contractors collecting, handling, storing, or transmitting Covered Information. Additionally, KPMG examined training compliance logs, meeting agendas, and attendance sheets maintained during Customer PII training sessions.
KPMG Test Results Summary	KPMG determined that SDG&E has developed company and department policies addressing the proper safeguarding of Covered Information. The organization is supported by a maturing Customer Privacy Program that has executive and management support, oversight, and visibility. Additionally, a process exists to respond to complaints/inquiries/disputes levied by customers related to Customer Privacy. Companywide training has been implemented but is not specific to data privacy and confidentiality of Covered Information. Additionally, data privacy and security training has not been rolled out to contractors hired through a temporary workforce solution company. KPMG also noted SDG&E provided the necessary information regarding Third Parties accessing Covered Information to the CPUC in their *Annual Privacy Report.*
Exception	Company-wide trainings provided during the covered period did not provide specific guidance to safeguard Covered Information. KPMG noted that management requires general Data Privacy training for specific, critical departments whose employees collect, use, store, or process Covered Information (e.g., CCC, Billing Operations, and Credit Operations).
Risk Level	Low
Risk Implication	SDG&E employees who collect, use, process, or store Covered Information may not understand or be aware of company policies and procedures for safeguarding sensitive information increasing the risk of misuse of data or a potential data incident.
Recommendation	SDG&E should provide specific guidance to safeguard Covered Information to all employees as part of company-wide training content, or at a minimum, provide specific guidance in training content required for those critical departments that collect, use, store, or process Covered Information.

SDG&E's Management Response to Covered Information Privacy and Security Assessment Report

Please see SDG&E's Management Response below.

September 15, 2014

Doron Rotman
Managing Director
KPMG LLP
Suite 2000
355 South Grand Avenue
Los Angeles, CA 90071-1568

Re: San Diego Gas & Electric's Response to KPMG's Covered Information Privacy and Security Assessment Report dated September 15, 2014

Dear Mr. Rotman:

On behalf of San Diego Gas & Electric ("SDG&E") we would like to thank you for the Professional Services KPMG provided in their external review and assessment of SDG&E's privacy and information security practices regarding Covered Information.

SDG&E engaged KPMG to complete this assessment in order to satisfy the California Public Utilities Commission's requirement to perform an independent audit of our compliance with the rules described in the Smart Grid Data Privacy Decisions (D.11-07-056 and D.12-08-045). We appreciate the rigor with which KPMG reviewed our privacy and security practices, validated where our programs are sound, and provided guidance on where our programs can do even better.

SDG&E has reviewed the exceptions contained in KPMG's Audit Report issued on September 15, 2014 and provides the following attached response.

Sincerely,

Lisa Davidson
Director, Customer Programs
San Diego Gas & Electric
Attachment

Any audit of any organization's business practices represents an opportunity to review and improve vital processes and technologies in order to better protect customer privacy. SDG&E welcomed the opportunity to review its privacy and security practices as we continually seek to enhance our programs. While KPMG's independent audit validated much of what our programs are doing to protect customer privacy, KPMG described four noteworthy findings in SDG&E's privacy and security audit. Below are SDG&E's responses to those findings.

CPUC Rule Number	Exceptions Noted by KPMG	SDG&E Management Response
CPUC Rule 6 **Use and Disclosure Limitation**	*New vendor contracts contain provisions requiring Third Parties to agree to safeguard Covered Information under policies, practices, and notification requirements no less protective than those under which the SDG&E operates.* *However, some existing, active vendor contracts may require a lower standard of safeguarding Covered Information consistent with the policies, practices, and notification requirements of the Third Party.*	SDG&E will work internally with all appropriate internal parties, including the Supply Management and Legal departments, to assess the population of contracts requiring update and develop an implementation plan for amending contracts to reflect the appropriate safeguarding of covered information.
CPUC Rule 8 **Data Security**	*No formal standards or procedures have been published to inform employees of requirements to protect data based on its classification.*	Although some company security standards do reference specific expectations regarding how to protect data based on its classification, SDG&E will work with its Information Security department in order to develop a matrix of protective guidelines for each classification level in order to clearly inform employees of recommendations to protect information based on its classification.
	The password configuration of a Third Party-hosted application, which stores commercial customer usage data, is not in line with the Sempra Password Standard. The application does not currently enforce password complexity requirements (e.g., minimum length, alphanumeric and special characters). In addition, the application team does not apply password complexity standards when creating master user account initially or when assigning an initial	As KPMG noted, SDG&E is already working with the vendor of this application in order to strengthen its password management system to meet minimum company standards, including complexity and temporary password resets on login.

CPUC Rule Number	Exceptions Noted by KPMG	SDG&E Management Response
	password to customer accounts. *SDG&E is currently working with the application vendor to update the application password configuration to be in line with the Sempra Password Standard requirements.*	
CPUC Rule 9 Accountability and Auditing	*While company-wide Customer Privacy training was developed it was not consistently rolled out to cover new employees hired after the training was initially launched, or certain contractors with access with Covered Information.*	In the summer of 2014, SDG&E implemented a new training system designed to reach contractors and external third parties that are required to take customer privacy training. To reach new hires after training has launched, the Office of Customer Privacy will work with its Information Security department to integrate a customer privacy module into standard Information Security training, which is part of the company's mandated annual compliance package. This should ensure new hires receive privacy training in a timely fashion after they join the company.

Appendix Detailed Test Procedures and Results

CPUC RULE 2 – Transparency (Notice)

Overall Conclusion	No Exceptions Noted

CPUC Rule 2	Rule Description	When Provided:
b		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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has documented policies addressing the provision of notice to customers of SDG&E's data collection and handling techniques.	1. a. Reviewed the internal privacy program documentation and noted that SDG&E adopts the Fair Information Practice Principles including the Principles Notice. The document states that SDG&E: ■ Will be transparent by providing notice regarding the collection, use, dissemination, purpose and maintenance of Personal Identifiable Information; ■ Will provide notice to customers on an annual basis regarding the Company's Privacy Practices. 1. b. Met with Manager, Office of Customer Privacy, and was informed that he includes a link to the SDG&E *Privacy Notice* and *Website Privacy Policy* in his email signature including those exchanged with internal and external recipients. The links provide individuals with notice of the company's privacy practices. 1. c. Reviewed documentation associated with *Changes to the Privacy Notice* and noted that changes will be driven and approved by the Law Department. Old copies of the *Privacy Notice* will be stored on a server and accessible upon demand if prior copies of the notice are requested by customers. The web team posts the final document to the website.	

2. Determine whether a procedure exists to ensure new customers receive notice of the company's privacy policy upon registration and annually thereafter. In addition, a procedure exists to track prior iterations of the privacy policy.	2. a. Met with Manager, Officer of Customer Privacy, and was informed that in addition to providing the *Privacy Notice* online, all customers receive a copy of the notice included as an *Annual Bill Insert* and new customers receive the materials as part of a *New Customer Welcome Package*. 2. b. Met with the Marketing Advisor and was informed that after a customer opens a new account with the CCC and turn-on eligibility is identified, a *Customer Welcome Package* is provided containing a *Cover Letter, Privacy Notice*, and *Safety Brochure*. The package is sent to customers via three methods: ■ Email to the email address provided on the account ■ Online at sdge.com/welcome ■ U.S. mail 2. c. Met with Billing Manager and Senior Service Advisor, Customer Operations and Manager, Remittance Processing, and was informed that the Bill Print group uses a Job code with the assigned print request to ensure the *Privacy Notice* is contained within customer mailings.	
3. Determine whether the SDG&E provides notice to customers on an annual basis and when signing up new customers as required by the CPUC regulation.	3. a. Reviewed the *Annual Bill Insert* included in bills from April and noted that it contains a section dedicated to SDG&E's Privacy practices and the safeguarding of Covered Information. 3. b. Reviewed a *New Customer Welcome Package Cover Letter* language and noted that a Cover Letter from the Manager, Customer Contact Center (CCC) includes the SDG&E *Privacy Notice* and provides the link to the SDG&E.com Welcome Site where customers can register for My Account to view their bill, usage, and ways to save.	

CPUC Rule 2	Rule Description	**Form:** The notice shall be labeled Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information (1) be written in easily understandable language, and (2) be no longer than is necessary to convey the requisite information.
c(1)-(2)		

Audit Procedures	Audit Test Results	Exceptions
1. Review SDG&E's methods for providing customers notice about their privacy and accessing the	1. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that SDG&E provides customers with information about the company's privacy practices on its website at http://www.sdge.com/privacy-notices.	

Privacy Notice.	1. b. Reviewed the *Website Privacy Policy* contained on the website at http://www.sdge.com/our-company/privacy-policy and noted that it provides web users with the reasons and methods for which the company collects information from the website. 1. c. Met with Manager, Officer of Customer Privacy, and was informed that in addition to providing the *Privacy Notice* online, all customers receive a copy of the notice included as an *Annual Bill Insert* and new customers receive the materials as part of a *New Customer Welcome Package*. 1. d. Reviewed emails sent from members of the Office of Customer Privacy and noted that their email signatures included links to the SDG&E *Privacy Notice* and *Website Privacy Policy*. The links direct to the company's privacy practices.	
2. Determine whether a procedure exists to review the readability of the privacy notice and make updates based on customer feedback related to readability and content.	2. a. Met with Manager, Office of Customer Privacy, and was informed that the *Privacy Notice* and *Website Privacy Policy* are reviewed by the Law Department prior to publication on the SDG&E website. 2. b. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it provides contact information where customers can provide comments or concerns regarding the notice.	
3. Determine whether SDG&E's Privacy Notice is written in an easy-to-understand language.	3. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* on the SDG&E website and noted that the language is written in laymen's terms and explains why SDG&E collects Energy Usage information, when it shares that information, and how consumers can access their Energy Usage information online. 3. b. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it is written at a Flesch-Kinkaid grade level of 14.0. Readers need to have a partial college education to fully understand the Notice. 3. c. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that customers have the options to view the notice in English, Spanish, Vietnamese, and Chinese. 3. d. Reviewed the *Website Privacy Policy* and noted that customers have the options to view the *Policy* in English, Arabic, Armenian, Farsi, Hmong, Khmer, Korean, Russian, Spanish, Tagalog, Thai, and Vietnamese.	

CPUC Rule 2	Rule Description	
d(1)-(4)		**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.

Audit Procedures	Audit Test Results	Exceptions
1. Understand how the regulatory requirements, management review and approval process works, including potential alterations of the Privacy Policies.	1. a. Met with Managing Attorney, Technology & Business Services. The role is responsible for interpreting any Privacy-related laws or regulations and defining the legal requirements of implementation. Most required changes to the *Website Privacy Policy* or *Privacy Notice* are communicated from the Law Department to the OCP. There are instances where new Business Processes require changes and those would be communicated from the OCP. 1. b. Met with Manager, Office of Customer Privacy, and was informed that if a new project requires a change to the SDG&E *Website Privacy Policy* or *Privacy Notice*, he would reach out to the Managing Attorney, Technology & Business Services, for guidance and approval of any updates. 1. c. Reviewed documentation associated with *Changes to the Privacy Notice* and noted that changes will be driven and approved by the Law Department. Old copies of the *Privacy Notice* will be stored on a server and accessible on demand if prior copies of the notice are requested by customers. The web team will post the final document on the website. 1. d. Reviewed redlined versions of *the Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* with edits and comments for updates prior to publication. The *Privacy Notice* replaced the March 20, 2012 version and was published on the SDG&E website.	
2. Inspect original and revision dates of policies to determine if actual updates/edits are made before approvals.	2. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it identifies SDG&E as the covered entity and has a revised effective date of October 15, 2012. 2. b. Reviewed the prior version of the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it includes an effective date of March 20, 2012.	

3. Determine how SDG&E informs customers of any alterations to the Privacy Notice and where prior versions will be made available to customers.	3. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it states: ▪ An online version of SDG&E's Privacy Notice along with any previous versions of this notice are located at sdge.com. We'll update this notice as necessary and when required by the CPUC and will inform customers of the update through information provided with the bill or our website. 3. b. Met with Manager, Officer of Customer Privacy, and was informed that updates to the *Privacy Notice* or *Privacy Policy* would be reviewed by the Law Department prior to publication and then placed on the website at sdge.com/privacy 3. c. Reviewed prior versions of the SDG&E *Privacy Notice* and *Privacy Policy* that were updated by revised versions.	
4. Examine whether SDG&E's Privacy Notices to identify whether the title and contact information (including email address, postal address and telephone number) of an official at the covered entity is indicated, who can assist the customer with potential privacy questions, concerns, or complaints.	4. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it provides information on how residential and commercial customers can contact the company via postal mail, email, and telephone. The Customer Privacy Office is identified as the point of contact for customer privacy concerns. 4. b. Reviewed the SDG&E *Website Privacy Policy* and noted that it provides information on how residential and commercial customers can contact the company via postal mail, email, and telephone.	

CPUC RULE 3 – Purpose Specification

Overall Conclusion	No Exceptions Noted

CPUC Rule 3	Rule Description	
a(1)-(3)		**Categories of Information:** (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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notice documents the (1) categories and purposes of Covered Information collected, used, stored or disclosed, (2) each category of Covered Information that is disclosed to Third Parties and purpose of disclosure, and (3) the identities of those Third Parties with whom Covered Information is shared for Secondary Purposes.	1. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it provides information to customers on (1) the Primary Purposes for which the company collects their Energy Usage data. These include: calculating billing information, electric and gas system planning, and planning, implementing and evaluating energy efficiency and demand response programs; the *Notice* informs customers on (2) the classes of Third Parties with which their information is shared: consulting organizations, engineering firms, and demand response and energy efficiency providers who are working with us to fulfill the Primary Purposes described above; Finally, the *Notice* states that it will seek customer consent prior to disclosure to a Third Party for a Secondary Purpose. Other reasons for disclosure include: 1) pursuant to a legal process (such as a warrant or subpoena), 2) to emergency responders in the case of imminent threat to life or property or 3) as ordered by the CPUC.	
2. Determine whether a procedure exists to ensure new customers receive notice of SDG&E's reasons for collecting, using, storing, or disclosing Covered Information.	2. a. See Rule CPUC Rule 2b. Audit Test Procedure 1 Audit Test Results. 2. b. Reviewed internal privacy program documentation and noted that a control exists for Purpose Specification stating that customers should be notified that their Personal Data will only be obtained, used, and shared for a specified and lawful purpose. All purposes should be disclosed in the *Privacy Notice*.	

3. Determine whether the SDG&E effectively monitors compliance with its collection, use, storage, and disclosure practices.	3. a. Met with CCC, Operations Support Supervisor, and was informed that CCC Operations Support will perform QA reviews of the Energy Service Specialists (ESS) including proper safeguarding of Covered Information and Customer PII. 3. b. Met with IT Audit Manager, Audit Services, and was informed about Audit Services and the two audits performed by Audit Services (SDG&E, SoCalGas) in 2012 related to Privacy and the protection of Customer PII including safeguards associated with collection, use, storage, and disclosure. Observed *Business Control Issues* (e.g., Findings) requiring Management Corrective Actions which are tracked by Audit Services to closure. 3. c. Reviewed sample *Customer Privacy and Security Audits* performed by Audit Services and noted that Audit Services reviewed SDG&E's compliance with different privacy and security safeguards in the information lifecycle. 3. d. Observed evidence that SDG&E uses an ERM tool to manage Third Party data sharing and Third Party data requests. 3. e. Reviewed sample *Privacy Impact Assessments (PIAs)* required by the OCP and noted that the use and impact of customer Covered Information is tracked during the PIA process and appropriate approvals are gained as needed. 3. f. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that the company reports instances of non-compliance with the *Privacy Decisions*. 3. g. Reviewed *Management Corrective Actions* prepared by Management and tracked by Audit Services in response to Business Control Issues identified during the SDG&E data privacy audit. Observed evidence that Audit Services tracked all Business Control Issues to closure.	

CPUC Rule 3	Rule Description	
b		**Retention Time:** The notice required under section 2 shall provide— The approximate period of time that Covered Information will be retained by the covered entity;

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notice addresses the retention of Covered Information.	1. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it contains a section labeled "Retention" which states: ■ SDG&E will keep your information only for as long as necessary to serve you and handle matters like billing disputes, inquiries and system planning. Retention periods vary based upon the specific circumstances and business needs, but will most typically be eight to ten years.	

CPUC Rule 3	Rule Description	
c(1)		**Customer Limitation:** The notice required under section 2 shall provide a description of (1) the means by which customers may view, inquire about, or dispute their Covered Information

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notice addresses customers' ability to view, inquire, or dispute their Covered Information or other PII.	1. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it identifies how customers may contact SDG&E with any questions or to find out how they can limit, view, or dispute their disclosed information. 1. b. Reviewed *SDG&E Bill Inserts* to customers which includes a link to the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted SDG&E provides customers with the opportunity to "find out how [they] can limit, view or dispute [their] information" by contacting SDG&E at: ■ Telephone 1-800-411-7343 ■ E-mail: CustomerPrivacySupport@Sempratilities.com ■ U.S. Mail: SDG&E, Attn: Customer Privacy P.O. Box 129831, San Diego, CA 92112-9831	

	1. c. Met with the Marketing Manager for SDG&E Residential Services and was informed that new residential customers receive a welcome package including a cover letter, the *Privacy Notice* and a brochure including contact information for questions. 1. d. Reviewed the *New Customer Welcome Letter* to new SDG&E customers and observed that the company discloses: ■ How customers can access their information online; ■ How customer privacy is managed, including a link to *SDG&E Privacy Notice* among other information.	

CPUC Rule 3	Rule Description	**Customer Limitation:** The notice required under section 2 shall provide a description of - (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.
c(2)		

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notices address customer choice and consent regarding data collection and handling practices, and the consequences for denying consent.	1. a. Reviewed the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it indicates that customers may limit their information by contacting SDG&E through mail, email or phone and provides appropriate contact details. 1. b. Reviewed the *Website Privacy Policy* and noted that it explicitly addresses customer choice for denying consent: ■ "You may choose not to provide any Personal Information and you will still be able to access most portions of the web site."	
2. Determine whether SDG&E's Privacy Notices address the explicit/implicit consent required to collect, use, and disclose Covered Information and other personal information.	2. a. Reviewed the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it addresses implicit customer consent. In addition, the *Notice* includes a link to My Account to view their information. 2. b. Walked through the *My Account Setup Process* on SDG&E.com and noted that customers must mark a check box acknowledging that they have read the *Terms and Conditions* which addresses customers' implicit customer consent for SDG&E to "collect, use, and disclose Covered Information and other personal information."	

3. Determine whether communication to individuals address the consequences of denying consent.	3. Reviewed *SDG&E Bill Inserts* to customers and noted a section informing about "*Protecting your privacy*". This section directs the customers to *SDG&E Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* (providing the web address, a phone number and email address. *SDG&E Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* indicates that customers may limit their information by contacting SDG&E through mail, email or phone and provides such contact details.	
4. Inspect SDG&E's systems where Customer Energy Usage Data is collected to determine whether customers' implicit or explicit consent preferences are captured (before data transfer).	4. Reviewed the *Website Privacy Notice* and noted that it includes an *Acceptance of Terms* clause that explicitly states, ■ "By using our web site or obtaining any product or service through our web site, you agree to the collection and use of information as set forth in this policy. If you do not agree to this policy, please do not use the web site."	

CPUC RULE 4 Individual Participation (Access and Control)

Overall Conclusion	No Exceptions Noted

CPUC Rule 4	Rule Description	
a(1)		**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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notice addresses the provision of access to individuals to their Covered Information.	1. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it provides customers with the link to My Account where they can view their usage data online. 1. b. Reviewed the *SDG&E.com Welcome Site* for new SDG&E customers and noted that it includes information for residential and business customers to sign up to view or receive alerts regarding their Covered Information. 1. c. Met with Manager, Office of Customer Privacy, and was informed that Commercial Customers use the kWickview tool to view their online interval usage. Additionally, customers can view Home Energy reports that are paper copies comparing their usage amounts to similar customers in their proximity. SDG&E also includes a link to Green Button on the website which allows customers to download up to 13 months of their personal electricity usage data through Green Button Download My Data.	
2. Determine whether SDG&E's internal policies describe the process for providing customers with access to their Covered Information.	2. a. Reviewed internal privacy program documentation and noted that the privacy program incorporates the Fair Information Practice Principles which include the principle *Access*. The documentation states that SDG&E: ■ Customers have the right to know about the collection of Personal Information, have access to their Personal Information, to be able to request correction if their Personal Information is incorrect and to challenge the denial of those rights. 2. b. Reviewed internal procedural documentation and noted that it provides SDG&E employees with step-by-step procedures for verifying the identity of anyone requesting customer information before granting access to the customer's Covered Information.	

3. Determine whether customers can access their Covered Information in a detailed, yet easy-to-read format.	3. a. Reviewed the Online Welcome Site for new SDG&E customers and noted that it includes information for customers to sign up for email or text alerts about their energy use and bill. 3. b. Reviewed the Energy Management Tool section on sdge.com and noted that it provides customers with information and video tutorials of the My Account feature and how they can view their usage: ■ Bill-to-Date Estimate ■ My Bill Highlights ■ When Does My Home/Business Use Energy? ■ How Does My Home/Business Use Energy? ■ My Neighborhood Comparison ■ How Does my Use Compare? 3. c. Met with Branch Office Supervisor, and was informed that customers can visit one of the five SDG&E Branch Offices to make payments, perform service requests, or receive a copy of their bill including usage data. 3. d. Reviewed a sample of a customer's My Account page and noted that customers are provided information on: ■ Energy consumption levels by time of day ■ The types of appliances using energy at the residence ■ How the customer's usage compares to other neighborhood customers ■ Estimated billing amount for the billing period 3. e. Reviewed a sample of a customer's portal page and noted that commercial customers are provided with their usage information by date range, summary and comparison statistics, and a comparison draft. 3. f. Reviewed the Green Button section of My Account and noted that customers can download their usage data for a specified date range. Customers can use Green Button Connect to authorize Third-Party vendors to receive their energy use information. 3. g. Observed customers at a Branch Office accessing their information by working with the ESS. 3. h. Observed ESSs at the Customer Contact Center (CCC) verifying customer identities while answering customer calls.	

CPUC Rule 4	Rule Description	Control:
b(1)-(3)		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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has a process in place for providing customers with access to grant and revoke authorization for secondary uses.	1. a. See CPUC Rule 5c. Audit Test Results 1. b. Met with the Manager, Office of Customer Privacy and noted that the company requires customer consent prior to the disclosure of customer information for Secondary Purposes, and that such consent would be confirmed and tracked before processing the request. 1. c. Inspected CISR form templates and executed samples of customer CISR forms and noted that a customer provided consent for disclosure of specific account information to a designated Third Party.	
2. Determine whether SDG&E has a process in place for customers to access their Covered Information and dispute its accuracy and completeness.	2. a. Met with Manager, CCC Business Process Team and was informed that CCC representatives provide customers with information on how they can update and correct their Personal Information on file with SDG&E. 2. b. Performed a walkthrough of the CCC and noted that ESSs can make updates to customer profiles upon request or necessity. 2. c. Inspected screenshots of My Account and observed that SDG&E provides customers with online access to their usage and other personal customer information, and provides customers with the ability to dispute potential incorrect/inaccurate information.	

3. Determine whether SDG&E has a process in place to make corrections or amendments to the collection, storage, use, or distribution of Covered Information upon a customer's request.	3. a. Reviewed the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it indicates that customers may view and dispute their information by contacting SDG&E through mail, email or phone and provides such contact details. 3. b. Reviewed the Smart Meter Opt-Out program available at http://www.sdge.com/residential/smart-meter-opt-out/smart-meter-opt-out-program for customers that do not wish to have advanced meters installed on their homes. The website provides guidance to customers and the necessary forms to complete and necessary contact information: ■ "Residential customers may choose between a smart meter and an analog meter. For your convenience there are multiple ways to opt-out of smart meter. i) Opt-out using our online form [provides link], ii) Submit your opt-out request by visiting one of our branch offices and iii) You may also opt-out by phone by calling at 1-877-357-8525." 3. c. Reviewed internal procedural documentation and noted that it provides guidance to ESSs on how customers may initiate the opt out process in the following ways: ■ Complete an online form at: http://sdge.com/residential/smart-meter-opt-out/smart-meter-opt-out-program. ■ Complete and return a form that will be included in the opt-out letter. ■ Emailing SDG&E at info@sdge.com. ■ Calling the SM direct number at: 1-877-357-8525 (Customers may provide opt-out requests verbally over the phone).The opt out request may only be submitted by the customer of record (primary or valid co applicant). ■ Visiting an SDG&E Branch Office. 3. d. Walked through the *My Account Setup Process* on SDG&E.com and noted that customers have the option to make corrections or amendments to their information. 3. e. See CPUC Rule 6e (1)-(3) Audit Test Results 2.	

CPUC Rule 4	Rule Description	
c(1)-(6)		**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 seven (7) days to appear and contest the claim of the person or entity seeking disclosure. (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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has procedures in place to ensure proper handling and documentation of any Covered Information data disclosures for legal reasons.	1. a. Reviewed the *Website Privacy Policy* and noted that it states that SDG&E may disclose Covered Information if it is necessary to comply with relevant laws or to respond to subpoenas or warrants. 1. b. Reviewed the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that customers are informed that SDG&E may share or release Covered Information pursuant to a legal process. 1. c. Reviewed the SDG&E Office Of Customer Privacy intranet website and noted that SDG&E has procedures in place for handling Third Party requests related to subpoenas. 1. d. Met with SDG&E Assistant General Counsel for Litigation and noted that SDG&E has procedures in place for handling and documenting Covered Information data disclosures for legal reasons.	

2. Inspect documentation regarding disclosure of Covered Information pursuant to a legal purpose to determine SDG&E properly handled the demand.	2. a. Reviewed internal tracking documentation and noted that a process is in place for SDG&E legal department to track incoming subpoena demands. These logs include the date the seven day notice was provided to customers, as well as the due date for the customer to respond to the notice, after which the SDG&E legal department would process the subpoena request. It was also noted that this tracking documentation has been updated to more adequately track the categories of data collected. 2. b. Met with SDG&E Assistant General Counsel for Litigation to review a sample of the seven day notices given to customers regarding subpoena demands for information and confirmed that a formal process for receipt, customer notification, tracking, and demand response is in place. 2. c. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that there were no non-compliance issues with the Privacy Rules or with contractual provisions required by the Privacy Rules which become known to SDG&E through its daily operations.	
3. Inspect the Annual Report submitted to the Commission to determine SDG&E reported the number of demands received for disclosure of customer data pursuant to situations of imminent threat to life or property and the number of customers whose records were disclosed.	3. a. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that during 2013, SDG&E received and answered 1,011 demands to disclose customer data pursuant to a legal process and the number of customers whose records was disclosed was 3,056. 3. b. Met with Manager, Office of Customer Privacy and learned that the *SDG&E 2013 Annual Privacy Report* includes the count of i) demands received for disclosure of Covered Information as defined in the regulation as well as ii) demands for non AM or usage related information. We were informed that SDG&E considers any sensitive customer data requests in their count for this reporting requirement, including PII, addresses and checking account information requests.	

CPUC Rule 4	Rule Description	**Disclosure of Information in Situations of Imminent Threat to Life or Property** 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).
d		

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has procedures in place to ensure proper handling and documentation of any Covered Information data disclosures for imminent threats to life or property.	1. a. Met with SDG&E Assistant General Counsel for Litigation and noted that SDG&E has procedures in place to handle disclosures of information in situations of imminent threat to life or property, where corporate security would receive the request and the legal department would be involved to handle it. In the case that the CCC would receive the request, it would be directed to corporate security.	

	1. b. Reviewed the SDG&E Office Of Customer Privacy intranet website and noted that SDG&E has procedures in place to disclosure customer information in response to emergency requests with threats to life or property. 1. c. Met with CCC Operation Support Manager and discussed the process for handling disclosure of information in situations of imminent threat to life or property.	
2. Inspect documentation regarding disclosure of Covered Information pursuant to an imminent threat to life or property to determine the number of demands and actual disclosures SDG&E engaged in, and whether SDG&E properly handled the demand.	2. a. Reviewed the *Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it informs the customers that SDG&E may share or release Covered Information to emergency responders in the case of imminent threat to life or property. 2. b. Reviewed the *Website Privacy Policy* and noted that it states that SDG&E may disclose Covered Information if it is necessary "to protect or defend the rights, property, or safety of our users, others, or ourselves."	
3. Inspect the Annual Report submitted to the Commission to determine whether the entity reported the number of demands received for disclosure of customer data pursuant to situations of imminent threat to life or property and the number of customers whose records were disclosed.	3. a. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that during 2013 SDG&E received one demand for disclosure of customer data pursuant to situations of imminent threat to life or property. 3. b. Met with SDG&E Assistant General Counsel for Litigation and Manager, Office of Customer Privacy and was informed that SDG&E reported one customer whose records were disclosed pursuant to the situation of imminent threat to life or property, and such disclosed records did not include Covered Information (only PII).	

CPUC RULE 5 Data Minimization

Overall Conclusion	No Exceptions Noted

CPUC Rule 5	Rule Description	
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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has Data Minimization procedures in place as they relate to the collection, storage, usage, and disclosure of Covered Information for Primary Purposes.	1. a. Reviewed the internal privacy program documentation and noted that the privacy program adopts the Fair Information Practice Principles including the Principles Collection/Minimization and Sharing. The documentation states: ▪ Collection/Minimization - Personal Information should only be kept for the length of time necessary to accomplish the specified purpose for which it was collected or as required by law, regulation or record retention guidelines. ▪ Sharing - under the Data Minimization guideline, only the minimum amount of Personal Information necessary to carry out the valid business purpose will be provided to a Third Party. 1. b. Reviewed internal privacy program documentation and noted that Data Minimization is a control incorporated into SDG&E projects to minimize the amount of customer information collected, used, and shared to that which is required to properly fulfill the business purpose for which it is collected, used, or shared. 1. c. Reviewed internal privacy program documentation and noted that the OCP defines Sensitive Customer Information and provides guidance on controls for protecting this information., 1. d. Reviewed internal training documentation and noted that SDG&E provides information on the distinction between Primary and Secondary Purposes and the requirements for collection, usage, and sharing of Covered Information for Primary Purposes. 1. e. Met with Manager, Office of Customer Privacy, and was informed that Data Minimization is a foundational principle of the SDG&E Privacy Program. The OCP reviews all Third Party data requests and projects for the data elements involved to determine the need for the collection, use, or disclosure of the data. The OCP has developed the internal tools to identify specific sensitive data elements, special requirements, and management approvals prior to inclusion in a project or disclosure to a Third Party.	

	1. f. Met with members of the SDG&E Records Retention team and was informed that classes of records are reviewed each year. 1. g. Observed evidence that SDG&E classifies Customer Energy Usage data as "Customer Sensitive" when combined with Customer Identifiable information. 1. h. Reviewed sample Third Party Data Requests within the ERM tool and noted that the requests identify whether they are for Primary Purposes. 1. i. Reviewed sample *PIAs* of projects performed in 2013 and noted that the Assessments were completed and approved in congruence with company policies.	
2. Determine whether SDG&E has Data Minimization procedures in place as they relate to the collection, storage, usage, and disclosure of Covered Information for Secondary Purposes.	2. a. Reviewed internal privacy program documentation and noted that SDG&E defines and details Secondary Purposes for the collection, storage, use or sharing of Personal Information. 2. b. Reviewed the internal training documentation and noted that SDG&E provides information on the distinction between Primary and Secondary Purposes and the requirements for collection, usage, and sharing of Covered Information for Secondary Purposes. 2. c. Reviewed the internal privacy program documentation and noted that SDG&E addresses the use of Covered Information for Secondary Purposes: ■ SDG&E will not, without the customer's prior consent, share Personal Information with Third Parties for Secondary Purposes. 2. d. Met with Manager, Office of Customer Privacy, and was informed that the OCP instituted a process to govern Third Party data requests. Requests for customer information require review and approval of the data request by different stakeholders within SDG&E. 2. e. Met with Specialist, Officer of Customer Privacy, and was informed that Third Party data requests for Covered Information for Secondary Purposes are either aggregated or require customer consent prior to disclosure. 2. f. Reviewed sample Third Party data requests and noted that the OCP captured whether customer information was being shared with a Third Party for Secondary Purposes and whether consent was required and obtained.	
3. Determine whether SDG&E implements Data Minimization across User Access roles to systems and applications where Covered Information is stored, used, or processed.	3. a. Reviewed internal procedural documentation and noted under the Need-to-Know Guidelines paragraph that Data Minimization is required for all information systems (including where Covered Information is stored, used or processed), and should be enforced on a need-to-know basis to prevent unauthorized access.	

	3. b. Reviewed internal procedural documentation and noted that Sempra Energy companies only retain records and non-records necessary for complying with legal, regulatory or financial requirements and for conducting business. 3. c. Reviewed internal privacy program documentation and noted that when collecting or sharing customer personal information, SDG&E seeks the minimum amount of information required to fulfill the business purpose for which it is collected or shared. 3. d. Met with various system owners and architects for nine systems that collect, store or process Covered Information and was informed that Information Security enforces Data Minimization principles on these systems through the use of user access profiles/roles or thin client (workstation only) installations. 3. e. Met with representatives of Billing Operations and was informed that Billing Operations controls system access to billing systems using different permission levels. 3. f. Inspected sample SDG&E systems and noted that user access roles have been implemented to help enforce Data Minimization over Covered Information stored, used, or processed in the application. 3. g. Observed screenshots of Branch Office users and noted that sensitive information is masked within the system. 3. h. Observed screenshots of CCC ESS users and noted that sensitive information is masked within the system.	

CPUC Rule 5	Rule Description	
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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's internal policies address a document retention policy covering all relevant aspects.	1. a. Reviewed internal procedural documentation and noted that the standards apply to the records of all Sempra Energy companies, regardless of the medium in which the records exist. Disposal of such records is subject to the policies and procedures as documented as well as legal hold orders. Sempra Energy's policy is to retain only those records that are necessary for complying with legal, regulatory, or financial needs and for conducting its business.	

	1. b. Reviewed internal procedural documentation and noted that it addresses corporate records definitions, retention schedules, the protection of records, records disposal and offsite storage. 1. c. Reviewed internal procedural documentation and noted that SDG&E sets forth the process for identifying and preserving records and non-records related to litigation or requests from government agencies. 1. d. Reviewed procedural documentation and noted that SDG&E has established retention schedules for each Department including the record series codes, record types, and official retention periods. 1. e. Reviewed internal privacy program documentation and noted that records retention is a privacy program control. Records retention controls include the following: ■ Personal data processed by the Company for any reason should not be kept any longer than is necessary for the business purpose for which it is being used ■ Records retention should follow the Company's retention schedule ■ Record retention schedules should support regulatory requirements 1. f. Reviewed internal privacy program documentation and noted that SDG&E addresses the retention of personal information.	
2. Determine whether the SDG&E retention policies are periodically reviewed and updated where necessary.	2. a. Reviewed internal records retention documentation and noted that Business Unit Records Officers are required to review the retention schedules annually to ensure that they are accurate and do not require adjustments. 2. b. Met with Business Controls and Compliance and was informed that the department VPs are required to review retention schedules annually and make necessary updates.	
3. Determine whether a management procedure exists to help ensure that documents are retained in compliance with company policies and that records are kept for only as long as reasonably necessary.	3. a. Met with Business Controls and Compliance and was informed that each year Sempra Energy and SDG&E undergo records cleanup for both electronic and hard copy records. Departmental Records Coordinators facilitate the effort and Directors and VPs of each Department must certify to compliance with the requirement. 3. b. Reviewed internal records retention documentation and noted that it provides the records clean-up schedule and dates by when Directors and VPs must certify their compliance. 3. c. Met with members of Application Services and Customer Operations and was informed that SDG&E implemented a process to purge customer data. 3. d. Reviewed sample management response prepared as part of Management Corrective Actions to an internal audit of SDG&E privacy practices and noted that a plan was developed to track purges of customer data.	

4. Inspect evidence of SDG&E documents complying with the record retention policies set forth by SDG&E.	4. a. Observed evidence of *Sempra Records Officer Certification of Records Management Compliance* for 2013 signed 10/2/2013. 4. b. Observed samples of signed VP and Director Certifications of Records Management Compliance for 2013.	
5. Inspect evidence that SDG&E destroys documents that are no longer necessary or when the appropriate retention policy ends.	5. a. Met with Branch Office Supervisor and was informed that a Third Party performs on-site pickup of records for shredding. 5. b. Met with CCC, Operations Support Supervisor and was informed that locked shred bins are located throughout the CCC floor and the Third Party will perform pickup for shredding upon request by SDG&E. 5. c. Observed evidence of shred bins at a Branch Office. 5. d. Observed evidence of shred bins on the SDG&E Billing department floor. 5. e. Observed evidence of shred bins throughout the Bill Print Remittance Center. 5. f. Observed evidence of customer data purging. 5. g. Reviewed a Third Party invoice and confirmed evidence of the destruction of records.	

CPUC Rule 5	Rule Description	
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.

Audit Procedures	Audit Test Results	Exceptions
1. Understand SDG&E's privacy policies to determine whether they: ■ Describe the practices related to sharing personal information (if applicable) with Third Parties and the reasons for information sharing,	1. a. Met with Manager, Office of Customer Privacy, and was informed that SDG&E only shares Customer Information with Third Parties if the customer provides consent through the CISR process. The CISR form can be valid for a specific period of time or indefinite as determined by the customer. The CISR form also limits information to be shared with only a designated, Third Party agent. Upon receiving the customer-signed CISR form, SDG&E will disclose the requested information for the designated purpose.	

■ Identify Third Parties or classes of Third Parties to whom personal information is disclosed.	1. b. Reviewed internal procedural documentation used by CCC as guidance for their operations. The document includes a detailed description of the practices related to sharing customer information with Third Parties and the process to follow. In addition, it indicates that: ■ "The customer of record must submit a signed authorization form or letter to the Company before customer information can be released to a Third Party", and contains a link to the form Authorization to: Receive customer information or act on a customer's behalf (also referred to as the CISR Form). 1. c. Reviewed the *Authorization to: Receive Customer Information or Act on a Customer's Behalf* and noted that the customer may authorize a Third Party as the agent to receive customer data such as billing records and usage data. This form is available in the SDG&E Online Help site. 1. d. Reviewed internal procedural documentation available on the SDG&E Office Of Customer Privacy intranet website for employees to provide to Third Parties for customer information requests. SDG&E collects the following information prior to the sharing of information: ■ Organization name, address, point of contact, phone number, email. ■ Scope and purpose of the request. ■ Specific customer information that is being requested. ■ Whether the project requires non-aggregated, customer specific information. ■ Period of the request. 1. e. Inspected executed samples of customer CISR forms and noted that a customer provided consent for disclosure of specific account information to a designated Third Party, identifying the length of the authorization (e.g., 12 months). 1. f. Reviewed internal privacy program documentation and noted that Data Sharing is a privacy program control. Data Sharing controls include the following: ■ Approval before sharing customer information with Third Parties ■ Customer Personal Data Purpose Specification 1. g. Reviewed internal privacy program documentation and noted that it addresses the sharing of Covered Information for Primary and Secondary Purposes.	

CPUC RULE 6 Use And Disclosure Limitation

Overall Conclusion	**Exception Noted:** New vendor contracts contain provisions requiring Third Parties to agree to safeguard Covered Information under policies, practices, and notification requirements no less protective than those under which the SDG&E operates. However, some existing, active vendor contracts may require a lower standard of safeguarding Covered Information consistent with the policies, practices, and notification requirements of the Third Party.

CPUC Rule 6	Rule Description	
c(1)-(3)		**<u>Disclosures to Third Parties</u> – (1) Initial Disclosures by an Electrical Corporation:** An electrical corporation 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. An electrical corporation 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 electrical corporation 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.	
Audit Procedures	**Audit Test Results**	**Exceptions**
1. Understand SDG&E's privacy policies to determine whether they: ■ Describe the practices related to sharing personal information (if applicable) with Third Parties and the reasons for information sharing, ■ Identify Third Parties or classes of Third Parties to whom personal information is disclosed.	1. See CPUC Rule 5c. Audit Test Results.	
2. Determine whether SDG&E informs customers that personal information is disclosed to Third Parties only for the purposes (a) identified in the notice, and (b) for which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation before data is disclosed to Third Parties.	2. a. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that it states that SDG&E may share CEUD with various other companies to serve its customers. In addition, it informs customers of the following: ■ "You can designate other companies to receive your information. When doing so, you should be diligent and only designate trusted Third Parties." ■ "Additionally, we may release Energy Usage information: 1) pursuant to a legal process (such as a warrant or subpoena), 2) to emergency responders in the case of imminent threat to life or property, 3) as ordered by the CPUC." 2. b. Reviewed the *Consent to Share Electrical and/or Gas Consumption Data* and noted that the customer explicitly agrees to allow the Utility to release to a Third Party Covered Information for a certain period of time (maximum of 13 months) when signing up for the Green Button program. In addition, the customer provides consent and agrees to the corresponding laws and regulations. This document is necessary for the release of Covered Information to Third Parties through the Green Button program which is managed by the company's Customer Energy Network.	

	2. c. Reviewed *SDG&E Bill Inserts* to customers which include a section for "Protecting your privacy" which directs the customers to *SDG&E Notice of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* (by the web site, phone or email) and noted that it indicates SDG&E informs customers that personal information may be disclosed to Third Parties.	
3. Determine whether SDG&E communicates specific instructions for handling personal information and the consequences of improper disclosure to the Third Party prior to disclosing the information.	3. a. Met with Portfolio Manager, IT/Telecommunications and noted that SDG&E contractually obligates Third Party vendors per their contract clauses to maintain the privacy of the information shared. Contractual provisions may be negotiated and modified on exceptional cases. 3. b. Inspected 24 SDG&E Contract Templates used by supply management for Third Party contracting and noted that the 24 documents contain a confidentiality clause governing the handling of personal information. 3. c. Reviewed internal procedural documentation and noted that SDG&E informs Third Parties that when accessing the utility's information it must only be used to perform SDG&E related work. In addition, SDG&E communicates to Third Parties that the information must be used in accordance with all applicable laws, regulations and contractual obligations. Suppliers are also notified that they must keep non-public information confidential and may only disclose non-public information if it is necessary for the performance of their work. 3. d. Reviewed a sample of executed internal agreement documentation and noted a nondisclosure section indicating that neither party may disclose any confidential information obtained, pursuant to the agreement to any Third Party: 3. e. Reviewed a sample contract between SDG&E and a Third Party and noted that it includes confidentiality and remedy clauses governing the handling of personal information by the Third Party.	
4. Understand whether Third Party contracting documentation is consistent with SDG&E's policies and procedures.	4. a. Reviewed internal procedural documentation governing Third Party contracting agreements. This documentation includes policies, procedures, and guidance for procurement purposes. It states that contractors will not be allowed to commence work until a valid contract is in place. 4. b. Reviewed internal security documentation and noted that it governs the protection of information when handing disclosures to Third Parties. This section includes specific procedures related to Third Parties contracting process, governing policies and requirements in order to safeguard customer privacy. 4. c. Reviewed internal privacy program documentation and noted that it includes sections for governing the process of sharing information and management of Third Parties. 4. d. See CPUC Rule 6(c) (1) (b) Audit Test Results. 4. e. Reviewed 24 SDG&E Contract Templates and noted that they contain language pertaining to the protection of Covered Information and the consequences of not performing accordingly.	New vendor contracts contain provisions requiring Third Parties to agree to safeguard Covered Information under policies, practices, and notification requirements no less protective than those under which the SDG&E operates. However, some existing, active vendor

	Noted there's an inconsistency between the guidelines (4. c,) and the contract templates (4. f.) reviewed with regards to the requirement that Third Parties agree to safeguard Covered Information under policies, practices and notification requirements no less protective than those under which the SDG&E operates. 4. f. Inspected a selection of Third Party contracts and noted the documentation includes provisions in line with those noted in the templates described in 4. e. above. 4. g. Met with Portfolio Manager, IT/Telecommunications to discuss Third Party contracting documentation. We were informed that each contract contains T&Cs that identify expectations from the Third Party and SDG&E internal contract sponsor/owner has the responsibility for the individual contract to ensure that the Third Party is in compliance with requirements.	contracts may require a lower standard of safeguarding Covered Information consistent with the policies, practices, and notification requirements of the Third Party.
5. Inspect sample evidence of acknowledgments/certifications from Third Parties regarding compliance with SDG&E's data privacy policies.	5. a. Inspected a sample of Third Party contracts and noted the documents include confidentiality, prohibition on Non-Public information sharing and remedies provisions in line with the contract templates reviewed. 5. b. Reviewed an executed *Energy Service Provider Service Agreement* and noted the last page of the Third-Party contract that shows an actual handwritten signature and serves as evidence of the Third Party's acknowledgement of compliance with confidentiality provisions included within. 5. c. Reviewed sample data disclosures within the ERM tool used to manage Third Party data sharing. Sampling demonstrated IS performed on-site reviews of certain high-risk Third Parties prior to customer data disclosure.	
6. Determine whether the entity has a process in place to review contract compliance for Third Parties receiving Covered Information.	6. a. Met with Portfolio Manager, IT/Telecommunications and found that SDG&E has a process in place to monitor contract compliance. It was stated that compliance with confidential customer information terms and conditions is the responsibility of the contract owner and it is tracked/monitored through the ERM system. KPMG performed a walk-through of the ERM system and confirmed its capabilities for monitoring Third Party contract status. In addition, Supply Management and the Legal department get involved in the contract negotiation as necessary and when non-compliance issues arise. 6. b. Reviewed internal privacy program documentation and noted that Data Sharing is a control within the Privacy Program framework.	

CPUC Rule 6	Rule Description	
d(1)-(3)		**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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E engages in Secondary Purposes, and determine if procedures are in place to: ■ Notify individuals and obtain their consent prior to disclosing personal information to a Third Party for purposes not identified in the Privacy Notice, ■ Document whether SDG&E has notified the individual and received the individual's consent, ■ Monitor that personal information is being provided to Third Parties only for uses specified in the privacy notice.	1. a. Reviewed internal privacy program documentation and noted SDG&E informs employees that: ■ Customers must provide consent prior to their Personal Information being used to carry out a Secondary Purpose. ■ Customers must have convenient access to their consent options and be provided with suitable mechanisms to change these choices at any time. ■ Change requests should be honored within a reasonable length of time. ■ Prior to analyzing or otherwise utilizing customers' Personal Information for Secondary Purposes, the customers' prior consent for such usage shall be obtained. 1. b. Met with Manager, Office of Customer Privacy and noted that the company requires customer consent prior to disclosure of customer information for Secondary Purposes, and that such consent would be tracked for processing the request. 1. c. Reviewed the SDG&E Office Of Customer Privacy intranet website and noted that the FAQs address Secondary Purpose information requests. 1. d. Met with Customer Programs Advisor and noted that the Office of Customer Privacy monitors customer information requests using an Enterprise Governance Risk and Compliance (ERM) tool.	
2. Determine whether customer consent authorizing use of Energy Usage data for Secondary Purposes is documented.	2. a. See CPUC Rule 6 e (1)-(3) Audit Test Results. 2. b. Inspected the ERM Tool used to manage Third Party data sharing and noted that the system indicates whether data is shared for Primary or Secondary Purposes.	

CPUC Rule 6	Rule Description	**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.
e(1)-(3)		

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether customers receive notice and must provide separate authorization if information is being used for a new Secondary purpose.	1. a. Reviewed internal privacy program documentation and noted that employees are required to receive customer consent prior to their Personal Information being used to carry out a Secondary Purpose. In addition, customers must have convenient access to their consent options and be provided with suitable mechanisms to change these choices at any time. Change requests should be honored within a reasonable length of time. 1. b. Met with Manager, Electric Load Analysis group and was informed about the CISR form process and the SDG&E parties involved. Noted that customers must provide separate authorization if information will be used for any Secondary Purpose.	
2. Understand how customers are notified of their right to revoke any previously granted authorization and the process to do so.	2. a. Reviewed the CISR form and noted that in order to complete it, customers must fill out explicit consent options and sign the acknowledgement clause. The CISR form contains the following clause regarding cancellation of authorization: ■ ″I understand that I may cancel this authorization at any time by submitting a written request". The duration of the authorization is limited to three years. 2. b. Reviewed the *Authorization or Revocation of Authorization to Receive Customer Usage Information* form and noted that customers have the option to grant and revoke authorization to Third Parties to receive usage information. The form notes that ■ "The purpose of this form is to allow you, the customer, to exercise your right to choose whether to disclose your personal natural gas interval usage data (i.e., hourly usage data) to a Third Party." 2. c. Inspected executed samples of customer CISR forms and noted that a customer provided consent for disclosure of specific account information to a designated Third Party, identifying the length of the authorization (e.g., 12 months).	

CPUC Rule 6	Rule Description	
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.

Audit Procedures	Audit Test Results	Exceptions
1. Inspect sample communications to see whether customers are notified of how they can cancel authorization for any Secondary Purposes.	1. a. Reviewed sample customer communications regarding how they are notified of the opportunity to cancel authorization for any Secondary Purposes. 1. b. See CPUC Rule 6. e (1)-(3). Audit Test Results 2. a-c.	

CPUC Rule 6	Rule Description	
g		**Availability of Aggregated Usage Data.** Covered entities shall permit the use of aggregated usage data that is removed of all PII 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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's Privacy Notice or internal policies address the use of aggregate information.	1. a. Reviewed internal privacy program documentation and noted that it addresses the use of Aggregated Information and states that Aggregated Data or Anonymized Data is not Personal Information. 1. b. Reviewed internal procedural documentation and noted that SDG&E is subject to the "15/15 Rule" which states that any aggregated or anonymized customer-specific information must be made up of at least 15 customers and a single customer's load must be less than 15% of an assigned category. 1. c. Reviewed internal privacy program documentation and noted that, when applicable, customer information is anonymized, aggregated or obfuscated so that it is not identifiable prior to being shared internally and with Third Parties.	
2. Determine whether SDG&E has a procedure in place to ensure aggregate information does not disclose or reveal	2. a. Met with Project Manager, Residential Services, and was informed that on occasion the Department receives requests from Third Parties for aggregated customer usage information. These normally include providing a residential or commercial complex's usage levels without identifiable customer information. When such requests are made we work closely with the OCP using the internal ERM system to ensure full compliance with Privacy requirements.	

specific Covered Information.	2. b. Met with Manager, Office of Customer Privacy, and was informed that SDG&E has implemented a process to assist with data sharing and data requests. 2. c. Reviewed internal procedural documentation and noted that SDG&E keeps track of the status of data requests including those for aggregate usage information and whether the request was fulfilled or denied.	

CPUC RULE 7 Data Quality and Integrity

Overall Conclusion	No Exceptions Noted

CPUC Rule 7	Rule Description	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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E's privacy policies address the quality of Covered Information and other customer PII.	1. a. Reviewed internal privacy program documentation and noted that a control associated with Data Use is Quality, Accuracy and Integrity of Collected Customer Personal Data. 1. b. Reviewed internal procedural documentation and noted that Sempra acknowledges the importance of accuracy within its records and disclosures. In addition this documentation indicates that Sempra Energy expects suppliers to have internal controls over operations and accounting records for accuracy purposes. 1. c. Reviewed internal privacy program documentation and noted that SDG&E addresses the specific rights customers have regarding the quality of, access to, and steps to correct Covered Information and other PII. 1. d. Reviewed internal privacy program documentation and noted that the privacy program incorporates the Fair Information Practice Principles which include the Principle Accuracy of Information, data integrity, and relevance.	
2. Inspect sample communication to customers to ensure whether SDG&E policies include customer data integrity.	2. a. Reviewed the *SDG&E Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that SDG&E provides customers with the opportunity to "find out how [they] can limit, view or dispute [their] information" by contacting SDG&E at: ■ Telephone 1-800-411-7343 ■ E-mail: CustomerPrivacySupport@Semprautilities.com ■ U.S. Mail: SDG&E, Attn: Customer Privacy P.O. Box 129831, San Diego, CA 92112-9831 2. b. Walked through the My Account setup process on SDG&E.com and noted that customers must	

	mark a check box acknowledging that they have read the *Terms and Conditions* which addresses customer's responsibility to provide accurate and up-to-date information. Specifically, SDG&E tells customers that, ■ "As a My Account user, it is your responsibility to ensure that the contact and other required information in your user profile is current and accurate, and updated promptly if necessary, including your name, address, phone number and email address. Changes can be made either within the My Account service or by contacting SDG&E's Customer Service by email or at 1-800-411-SDGE (7343)." 2. c. Reviewed internal privacy program documentation and noted that SDG&E addresses internal data integrity, accuracy, and relevance.	
3. Determine whether procedures are in place that: ■ Edit and validate personal information as it is collected, created, maintained, and updated, ■ Specify when the personal information is no longer valid.	3. a. Met with CCC Operations Support Supervisor and was informed that ESS's authenticate customers during the call intake process using their internal validation process. Customers have the opportunity to update the information on file that is no longer valid. 3. b. Met with Senior Accountant, Lead on Records Manager to discuss policies and procedures for managing confidential customer information and its destruction when is no longer valid. It was stated that each record containing confidential information is associated with a specific code from a code listing provided by corporate. According to the code given to the document, the record will fall under a specific time range to be retained and would be destructed after that date. 3. c. Reviewed internal privacy program documentation addressing PII retention and the laws and regulations dictating their collection. 3. d. Met with Manager, Internal Audit and noted that data privacy and security areas are assessed and considered annually by Audit Services. SDG&E had been recently subject to audits which included security in their scope. 3. e. Reviewed internal audit reports and noted that privacy and security controls were reviewed in the audit. Business control issues were identified and management corrective actions were provided with corrective action plans to resolve each item. 3. f. Reviewed *Management Corrective Actions* prepared by Management and tracked by Audit Services in response to Business Control Issues identified in data privacy audits Observed evidence that Audit Services tracked all Business Control Issues to closure. 3. g. Reviewed internal procedural documentation and noted that SDG&E's Smart Meter data management system has built in controls to validate energy usage levels.	
4. Inspect sample evidence to	4. a. Reviewed internal procedural documentation and noted that SDG&E Company Information shall	

ensure that procedures are in place that help ensure personal information is sufficiently relevant for the purposes for which it is to be used and to minimize the possibility that inappropriate information is used to make business decisions about the individual.	be used solely for authorized business purposes. 4. b. Reviewed internal privacy program documentation and noted that SDG&E informs its employees about the procedures in place to ensure personal information is sufficiently relevant for the purposes for which is being used. 4. c. Met Manager, OCP and noted that during the My Account registration process SDG&E only collects the necessary data fields. 4. d. Met with Billing Manager and Senior Service Advisor, Customer Operations, and was informed that the Billing Department is responsible for correcting inaccurate Smart Meter data reads. 4. e. Reviewed internal procedural documentation and noted that the Smart Meter performs edit checks for validity, completeness, and reasonableness of data.	

CPUC RULE 8 Data Security

Overall Conclusion	**Two Exceptions Noted:** ■ No formal standards or procedures have been published to inform employees of requirements to protect data based on its classification. ■ The password configuration of a Third Party-hosted application, which stores commercial customer usage data, is not in line with the Sempra Password Standard. The application does not currently enforce password complexity requirements (e.g., minimum length, alphanumeric and special characters). In addition, the application team does not apply password complexity standards when creating master user accounts initially or when assigning an initial password to customer accounts. SDG&E is currently working with the application vendor to update the application password configuration to be in line with the Sempra Password Standard requirements.

CPUC Rule 8	Rule Description	
a		**Generally** Covered entities shall implement reasonable administrative, technical, and physical safeguards to protect Covered Information from unauthorized access, destruction, use, modification, or disclosure.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has documented policies addressing security provisions for Covered Information.	1. Met with relevant stakeholders from Information Security & Information Management and inspected the documentation provided. Noted that the following policies/procedures/standards/guidelines are in place to address security provisions for SDG&E in general, including Covered Information: ■ *Risk assessment and treatment* – an overall network threat and vulnerability assessment is performed by the Information Security group as well as continuous threat and vulnerability identification and remediation. The threat and vulnerability process is formally documented. In addition, quarterly updates are provided to the CIO on SDG&E's security posture, including risk and remediation status. ■ *Security policy* – An Information Security Policy is in place and published on the company's intranet site, accessible to all SDG&E employees. Additional supporting Information Security policies (e.g., acceptable use policy), standards, procedures and guidelines are also published on the company intranet site. ■ *Organization of Information Security* – a formal Information Security organization has been established and serves SDG&E. The Information Security group consists of sub specialist groups	

	who focus on specific aspects related to securing the organization's IT network, systems and data. ■ *Asset management* – Formal procedures and requirements have been established to identify and record the security features and controls used to protect Sempra information assets. Requirements are in place for the monitoring and tracking of assets. It was also noted an Information Security Acceptable Use Policy is in place to govern the use of information assets. ■ *Human resources security* – Roles and responsibilities have been defined for owners and users of information assets. A requirement for Security Awareness Training has also been established. ■ *Physical and environmental security* – Physical and Environmental Security requirements are formally documented. ■ *Communications and operations management* – Requirements pertaining to communications and operations management are formally documented. ■ *Access control* – Access Control requirements are formally documented. ■ *SDLC: Information systems acquisition, development, and maintenance* – Requirements for the acquisition, development and maintenance of information systems, hosted either internally or by vendors, have been defined. ■ *Information security incident management* – Information Security Incident Management related to Covered Information has been formally documented. ■ *Business continuity management* – Business Continuity Management procedures have been formally documented. ■ *Compliance* – The requirement for compliance with applicable privacy legislation and regulations has been formally documented in the company's information security policy. Detailed compliance requirements are also formally documented in additional policies available on the company's intranet.	
2. Determine whether SDG&E privacy policies and procedures cover protection of electronic and print media containing Covered Information from unauthorized access, destruction, use modification or disclosure.	2. a. Procedures are in place that require the protection of information commensurate with the asset value, requirements of applicable law and assessed risk. Controls Owners and Managers are required to implement and maintain security features and controls to protect information and information systems. 2. b. Contracts are required for authorizing Third Party access to company information, where legally required or otherwise deemed advisable by an appropriate risk owner, security measures to mitigate risk of unauthorized acquisition, modification, or destruction. 2. c. Specific requirements around access control to electronic data through systems as well as print media have been established.	

3 Determine whether a management procedure exists to monitor compliance with the security provisions in the policy and instances of noncompliance are identified and remediated.	3. a. Formal guidelines have been established for monitoring compliance with security provisions. 3. b. Observed that instances of noncompliance are formally documented and sent to Information Security management for compliance monitoring. 3. c. A risk exception process has been established for cases where compliance requirements cannot be met due to technical limitations. Risk exceptions and their mitigation and remediation plans are formally documented.	
4. Review evidence that SDG&E's policies on Data Security are communicated to internal employees and contractors who have access to Covered Information.	4. a. Reviewed an internal company website and noted that all policies on data security are published on the SDG&E intranet site which is accessible by all SDG&E employees and contractors. 4. b. Reviewed the *Website Privacy Policy* and noted the data security policy for Covered Information detailed in the document.	
5. Determine whether SDG&E informs customers how it secures their Covered Information.	5. a. Reviewed the *Website Privacy Policy* and *Privacy Notice* and noted that they are shared with website visitors to communicate how information is collected, used/shared, and protected when visitors view the SDG&E website. 5. b. Reviewed the *Notice Of Accessing, Collecting, Storing, Using, and Disclosing Energy Usage Information* and noted that procedures have been established for using/sharing and retaining customer data and have been communicated to customers.	
6. Determine whether a management procedure is in place to monitor whether SDG&E manages its security program to help ensure the protection of Covered Information.	6. a. Information Owners are expected to establish security requirements for data and information, and to ensure that security features and controls are maintained for the duration of processing and storage of data and information, and that information retention/recovery plans are in place. 6. b. A quarterly security briefing is provided to the CIO providing reports on specific controls related to the protection of Covered Information.	
7. Review SDG&E relevant policies to determine if entity incorporates security into their SDLC.	7. a. Reviewed documentation and noted that security is incorporated into the various phases of the IT product lifecycle. 7. b. Formal documentation is prepared as part of the SDLC process in which the resolution of privacy risk and compliance changes in new and updated systems and business processes are identified and facilitated. 7. c. If Information Security is not incorporated during the system implementation, a formal risk exception must be filed, which should include risk mitigation measures and remediation plans.	

	7. d. All system changes for SDG&E are assessed by the Privacy Team.	
8. Determine whether SDG&E uses appropriate facility entry controls to limit and monitor physical access to systems and locations where Covered Information is processed and stored.	8. a. Controls for limiting access to facilities are have been identified and formally documented. All employees are required to wear physical identification and systems are in place to restrict physical access to authorized locations and work areas. 8. b. A formal process for requesting, obtaining approval and granting physical access to restricted areas is documented. Access is also reviewed periodically. 8. c. Observed reasonable physical access controls have been implemented at facilities where systems or physical records containing Covered Information are hosted or stored. 8. d. A form of ID verification was not required when signing in as a visitor at some locations, but an authorized employee was required to escort the visitor.	
9. Determine whether SDG&E has implemented procedures for protecting Covered Information including controls for physically securing all media.	9. a. Formal requirements and guidelines have been established that require all Sempra Energy Confidential and Restricted Information, including Covered Information and customer PII to be encrypted at rest or in transit through commercially available products. This includes encryption of physical media in storage or in transit, including but not limited to offices, desktops, data centers, media libraries, backup centers and field locations. 9. b. Observed reasonable physical access controls at buildings that host customer operations or Covered Information systems.	
10. Inspect whether physical records containing Covered Information are stored in locked cabinets or rooms restricting unauthorized access.	10. Observed at various customer operations sites that physical records containing customer PII are physically locked in a secure location or securely destroyed once no longer needed.	
11. Inquire of SDG&E's personnel to gain an understanding of the logical control procedures in place to prevent unauthorized access to Covered Information.	11. a. Systems are configured to prevent unauthorized access to Covered Information through various access controls: ■ authentication parameters (unique user ID and password); ■ strong password configuration based on internally established standards; ■ restricted access based on roles or responsibilities; ■ two-factor authentication. 11. b. The network is logically segregated to restrict access to the required network segments and systems or applications based on roles and responsibilities. The firewall combined with a number of	The password configuration of a Third Party-hosted application, which stores commercial customer usage data, is not in line with the Sempra Password Standard. The

	switches and routers are used to restrict access to specific network segments and systems. 11. c. Met with System Owners of a customer-facing application and was informed that password parameters for the application do not currently comply with the Sempra password standard and does not enforce any complexity or minimum password length. The application is a vendor supported application and Sempra does not have access to the source code. SDG&E is in the process of working with the vendor to update the application configuration to be aligned with the Sempra password standard. It was also noted per inspection of the application User ID Procedure document that a user's last name is typically used as the initial password.	application does not currently enforce password complexity requirements (e.g., minimum length, alphanumeric and special characters). In addition, the application team does not apply password complexity standards when creating master user accounts initially or when assigning an initial password to customer accounts. SDG&E is currently working with the application vendor to update the application password configuration to be in line with the Sempra Password Standard requirements.
12. Inspect evidence that logical controls are in place to prevent unauthorized access to Covered Information including user access provisioning and deprovisioning.	12. a. Formal access management guidelines are in place including the following: ■ All new user accounts or changes to existing accounts have to be approved by the control owner. ■ The principle of "least privilege" should be applied for all user accounts. ■ Segregation of Duties should be enforced for roles to avoid individuals submitting requests from having the access rights to approve their own requests. ■ Users have to be authenticated to systems by a unique user ID and password. Users should be locked out after a number of unsuccessful login attempts and their identity verified if they request their password to be reset. ■ Passwords must enforce strong criteria in line with internal standards.	No formal standards or procedures have been published to inform employees of requirements to protect data based on its classification.

	■ Accounts for terminated employees or employees changing roles should be updated timely. Unused or inactive accounts should be disabled. ■ User account reviews should be performed periodically. 12. b. Noted that systems containing Covered Information have reasonable user authentication and authorization measures in place 12. c. Noted that user access is approved and assigned in line with job responsibilities. 12. d. Noted that user access reviews are periodically performed for Covered Information systems and access updated in line with management requests.	
13. Review SDG&E's relevant policies to determine if physical controls are in place protecting Covered Information.	13. A formal policy has been established listing the physical controls implemented to protect Covered Information.	
14. Inquire of SDG&E's personnel to gain an understanding of the controls protecting physical access to systems storing Covered Information.	14. Inquired of Information Security management and noted that physical access to systems storing Covered Information is controlled through various physical controls that restrict access to specific locations based on approved clearance required by job responsibilities. It was also noted that all visitors are required to sign-in and be escorted when accessing restricted areas. In addition all employee access to restricted areas are reviewed periodically to ensure access is appropriate and approved.	
15. Inspect evidence that physical access to sites and systems storing Covered Information is monitored and restricted.	15. Per inspection of facilities hosting Covered Information systems it was noted that physical controls are put in place to monitor and restrict access to Covered Information.	
16. Review SDG&E's relevant policies to determine if environmental controls are in place.	16. Reviewed internal security documentation and noted that requirements have been established for protecting Sempra information assets against risks related to heat, fire, theft, smoke, water, explosion, dust, vibration, chemical effects, electrical interference, power disruption, and electromagnetic radiation, power and physical tampering.	

17. Inquire of SDG&E's personnel to gain an understanding of the environmental controls to protect systems storing Covered Information from natural disasters and environmental disasters (such as fire or flooding).	17. a. Inquired of Information Security management and noted that environmental controls are in place to protect physical systems storing Covered Information from natural and environmental disasters. 17. b. Noted at facilities hosting Covered Information systems that reasonable environmental controls are in place to protect Covered Information from natural and environmental disasters such as fire or flooding.	
18. SDG&E has the ability to transfer data to Third Parties using secure channels.	18. a. Large file transfers to vendors or partners should be completed through the in-house file transfer application. Formal requirements have been defined for the transfer of confidential data, which includes processes and tools to ensure the privacy and integrity of sensitive information, specifically movement of data between networks using secure, authenticated, and encrypted mechanisms. 18. b. An additional data security tool is in the process of being implemented to monitor transfer of data to Third Parties. 18. c. Met with various System Architects and noted that customer usage data for customer energy efficiency programs are shared with Third Parties using in house file transfer applications.	
19. SDG&E has deployed an automated tool on network perimeters that monitors for Customer PII, keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting Information Security personnel	19. a. Automated tools and techniques have been implemented to filter and block specific file types or attachments sent or received via email based on a predefined policy and configuration standard. 19. b. An additional data security tool is currently in the process of being implemented to further help prevent unauthorized attempts to exfiltrate data across network boundaries and block transfers while alerting information security personnel.	
20. SDG&E has deployed an automated tool on workstations that monitors for Customer PII, keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data to removable media and block such transfers	20. a. An additional data security tool is currently in the process of being implemented to help monitor for customer PII, keywords and other document characteristics related to unauthorized attempts to exfiltrate data to removable media and blocking transfers while alerting information security personnel. 20. b. A formal procedure has been defined for alerting information security personnel in the event of a potential event on a workstation. The procedure specifies the following information to be captured for the event. The procedure specifies the following information to be captured for the event: ■ specific information of impacted systems or applications	

while alerting Information Security personnel	■ specific information disclosed (i.e., customer name, account numbers, etc), ■ system ownership (Sempra or Third Party (if applicable)), and ■ status of information (encrypted or unencrypted).	
21. SDG&E has controls in place so that users cannot disable and modify security products or services.	21. a. Users are prohibited from circumventing security features or controls that are put in place to protect the corporate computing environment from intrusion, compromise, and/or misuse. 21. b. Noted that users do not have access to disable and/or modify security products or services.	
22. SDG&E understands the current threat landscape and potential threats to the organization by leveraging multiple threat feeds.	22. a. Potential threats and risks are identified using a variety of information sources including SANS, local law enforcement agencies, cyber security and industry specific newsfeeds. 22. b. A formal and continuous threat management and risk assessment process is in place using a combination of tools and procedures. 22. c. Vulnerabilities and threats are assessed to determine the risk to the environment and if identified to have an impact, a risk assessment will be formally documented and a priority assigned. If the risk cannot be remediated due to limitations or restrictions, a Risk Exception will be completed and formally documented. Vulnerabilities are remediated by the relevant team that owns the application. 22. d. A formal report is issued to management on a periodic basis providing an overview of the organization's threat landscape and risks, as well as key metrics for the Cybersecurity areas that are monitored.	
23. SDG&E scans source code for bugs and vulnerabilities before moving it into production	23. A preliminary automated code scan is always completed before new applications or code changes are deployed into the production environment. There is also a process to determine the severity of the system or the change which will prompt a penetration test on the source code. If Information Security is involved in the test phase of a system change or implementation, a source code scan is completed at this point as well. Periodic vulnerability scans of the entire network is also performed, which will scan source code changes that were not scanned for vulnerabilities prior to moving it into production.	
24. SDG&E's development/test environments are separate from the production environment, with access control in place to enforce the separation.	24. a. Development and test environments are hosted on different servers than production systems containing Covered Information. Access to the different servers is segregated using logical access controls. 24. b. A formal change control process is in place to manage changes to Covered Information system production environment source code. Changes to production source code are controlled using a source code repository tool in some cases.	

25. Determine whether SDG&E does not use Production Covered Information for testing or development. Test data and accounts are removed before a production system becomes active.	25. Production Covered Information is typically not used for testing and development activities. If required for testing activities, sensitive data will be masked.	
26. Determine whether SDG&E utilizes a Data Masking tool to limit access to and protect Covered Information and other PII.	26. Observed during a site walkthrough of a number of customer operations facilities and system samplings that sensitive customer information data fields are masked.	
27. SDG&E's web applications should use encryption when transmitting sensitive data across the network.	27. a. Formal standards have been established which require that Sempra Energy Confidential or Restricted Information being transmitted over any untrusted communication network should be sent in encrypted form. Encryption of Sempra Energy Confidential and Restricted information in transit is achieved via commercially available encryption products, 27. b. All Covered Information and customer PII data are transmitted either internally or to Third Parties using an internal secure transfer method, which encrypts the data in line with the Sempra encryption standards. 27. c. A formal standard for wireless access to internal networks, systems, applications and data is in place to help ensure secure transfer of data through wireless networks in line with strong encryption practices.	
28. Determine whether SDG&E has implemented an Intrusion Detection system within the environment to detect and generate log messages detailing events.	28. An Intrusion Detection System (IDS) has been deployed on the network and is configured to identify possible intrusions based on specific configured rules. When a potential event is identified, the Security Operations Center is notified and the incident is formally documented and tracked through resolution following the incident response procedure	

29. Determine whether SDG&E has implemented an Intrusion Prevention system within the environment to detect events and reject packets.	29. An Intrusion Prevention System is in place and is configured to detect and reject packets based on predefined and configured rules.	
30. Determine if SDG&E allows limited access to network resource to vendors and 3rd parties.	30. a. Contracts authorizing Third Party access to information or systems include security measures to mitigate the risk of unauthorized acquisition, modification or destruction. 30. b. A formal standard has been established requiring vendor access to internal systems to be limited to the duration of the contract. Specific requirements have been defined for boundary protection and design, specifically external connections into the network or to network resources, including limiting incoming communications only from authorized sources routed to authorized destinations using firewalls and routers. 30. c. A formal standard has been established requiring vendor access to internal systems to be limited to the duration of the contract. Specific requirements have been defined for boundary protection and design, specifically external connections into the network or to network resources, including limiting incoming communications only from authorized sources routed to authorized destinations using firewalls and routers.	
31. Determine if SDG&E has a formal process for approving and testing all network connections and changes to the firewall and router configurations	31. a. All connections to and changes to the production firewall environment are tested in the non-production environment designated by the responsible parties. Changes not able to be tested prior to implementation will be validated in the production environment. All normal changes must have a test plan and/or post implementation validation plan prior to receiving change management authorization. High risk changes will be discussed at the Change Advisory Board meeting and will need to include a test plan and a post implementation validation plan to be reviewed with the board prior to authorization. 31. b. Changes made to the firewall must be formally documented and approved by the Information Protection Manager and comply with current Change Management Procedures. 31. c. The security configurations of network devices including firewalls, routers and switches are tracked using a configuration management and change control process.	

32. Determine whether SDG&E's firewall performs stateful inspection (dynamic packet filtering) to restrict network access at the header level.	32. The firewall is configured to perform stateful inspection.	
33. Determine if SDG&E has implemented a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	33. A formal standard has been established with requirements for the DMZ, including the use of a combination of network devices such as a firewall and routers to govern DMZ traffic and prevent unauthorized access to the internal network and systems.	

CPUC Rule 8	Rule Description	
b		**Notification of Breach:** A covered Third Party shall notify the covered electrical/gas corporation 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 electrical/gas corporation or by a covered Third Party, the covered electrical/gas corporation 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, electrical/gas corporations shall notify the Commission's Executive Director of security breaches of Covered Information.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has documented incident response and breach management procedures in place including roles and responsibilities, testing and training, incident classification and logging, remediation, and program updates.	1. a. Reviewed internal security documentation and noted that a process is in place for employees to escalate a security incident if they suspect an activity has occurred. 1. b. Based on the incident management policy and procedures, all incidents are formally documented, logged and tracked. Incidents are assigned a severity and communicated to the relevant incident response team members as defined in the procedure document, who will perform the responsibilities based on their assigned role. 1. c. Inquired of management and was informed that the company is in the process of reviewing and updating the incident response policy. 1. d. Met with Manager, Office of Customer Privacy, and was informed that that a corporate incident response process exists to track and escalate privacy incidents. 1. e. Inquired of management and was informed that Information Security developed its Incident	

	Response program based off Information Security best practices. 1. f. Met with Sempra Vice President – Compliance and Governance and Corporate Secretary, and was informed management receives updates on data security and breach management. 1. g. Met with Director, Customer Operations, and was informed that customer data privacy incidents receive management-level attention. 1. h. Reviewed internal privacy program documentation and noted that it addresses the reporting of unauthorized releases of customer information. 1. i. Reviewed internal security documentation and noted that Third Parties are required to report potential breaches and data incidents.	
2. Determine whether SDG&E's management has adequately reviewed the incident review process in place.	2. a. Inquired of Information Security management and was informed that the incident response policies are reviewed annually. 2. b. Observed evidence that incident response documentation was reviewed in August 2013. 2. c. Reviewed management proposed updates to the existing incident response documentation. 2. d. Met with Senior Vice President/Chief Information Officer Sempra, and was informed that information security works in collaboration with the individual Privacy teams and legal groups responsible for ensuring appropriate handling of data breach incidents.	
3. Determine whether SDG&E can perform forensic analysis in the instance of a Customer PII breach.	3. a. Reviewed internal incident management documentation and noted that tools exist to analyze potential data incidents. 3. b. Inquired of Information Security management and was informed that a specific suite of tools is in place for forensic analysis activities, including tools to preserve evidence and identify the impact of a breach. 3. c. Reviewed internal incident response documentation and noted that roles in the incident response process are defined. 3. d. Inquired of Information Security management and was informed that the Information Security group maintains a close relationship with local law enforcement agencies (e.g., San Diego Police Department), the FBI and the Department of Homeland Security and have a process in place to connect with law enforcement if required.	
4. Inspect sample evidence of breach incidents for the last 12 months.	4. a. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that SDG&E reported two incidents involving a breach of Covered Information in 2013. 4. b. Observed evidence that SDG&E tracks potential data incidents from identification to closure	

CPUC Rule 8	Rule Description	**Annual Report of Breaches:** In addition, electrical corporations 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 electrical corporation or by a Third Party.
c		

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E tracks the reporting requirement and assigns compliance to the appropriate department.	1. a. Met with Manager, Office of Customer Privacy and was informed that the OCP is responsible for collecting the information to complete the *CPUC Annual Privacy Report*. The OCP uses a Report template which contains a table of all the report requirements and step-by-step instructions on the appropriate stakeholders to contact to collect the data elements. 1. b. Reviewed *Privacy Decision compliance tracking* documentation and noted that Information Security & Information Management provided information to the Customer Privacy Team on breach information for the Annual Privacy Report. 1. c. Inquired of Information Security management and was informed that the company can run reports related to Covered Information incidents. 1. d. Met with Manager, Office of Customer Privacy and confirmed that no breaches affecting 1,000 or more customers occurred and that there were two incidents affecting Customer Usage Information occurred during 2013 as noted in the *Annual Privacy Report*.	
2. Determine whether SDG&E filed its Annual Report to the CPUC as required by the Privacy Decision.	2. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that it was submitted to the CPUC on April 30, 2014 by Director, Regulatory Affairs. The report identified: ■ No breaches affecting 1,000 or more customers. ■ Two incidents within the calendar year affecting Covered Information, whether by the covered electrical corporation or by a Third Party.	

CPUC RULE 9 Accountability and Auditing

Overall Conclusion	**Exception Noted:** While company-wide Customer Privacy training was developed it was not consistently rolled out to cover new employees hired after the training was initially launched, or certain contractors with access to Covered Information.

CPUC Rule 9	Rule Description	
a		**Availability:** 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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E has external Privacy Notices to provide to its customers.	1. a. Reviewed the SDG&E website at www.sdge.com/privacy and noted that there are two different privacy statements: ■ *Website Privacy Policy* - The *Privacy Policy* for the SDG&E website informs customers as to how their information is collected, used, and disclosed based on their activities on the website. ■ *Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information* - The Notice as required by the *Privacy Decision* informs customers to how SDG&E collects, stores, uses, and discloses their Covered Information. 1. b. Met with Manager, Office of Customer Privacy, and was informed that SDG&E has two separate external Privacy Policies for customers. The *Website Privacy Policy* has existed for many years as required by the "California Online Privacy Protection Act" and relates to how SDG&E collects, uses, and discloses information from website users. The *Notice Of Accessing, Collecting, Storing, Using,*	

	and Disclosing Energy Usage Information was developed in response to the *Privacy Decision* and covers SDG&E's practices associated with Covered Information.	
2. Determine whether SDG&E has internal privacy and security policies.	2. a. Met with Manager, Office of Customer Privacy, and was informed that SDG&E has internal policy related documentation that governs the appropriate safeguards of information. The documentation covers the collection, use, retention, and disclosure of information. 2. b. Met with Manager, Office of Customer Privacy, and was informed that SDG&E developed a *PIA* to determine the impact of projects on customer privacy. 2. c. Met with Managers, Billing Operations, and was informed that Billing Operations as part of Customer Service is subject to Sempra and SDG&E policies and procedures. Billing Operations also maintains department-specific policies governing the protection of customer information that all employees must certify to annually. 2. d. Reviewed internal privacy program documentation and noted that the foundational principles of the SDG&E Privacy Program are addressed. The program is based on the Fair Information Practice Principles and Generally Accepted Privacy Principles (GAPP) and adopts Privacy by Design (PbD) as an approach to embed privacy within the environment. Contact information for the OCP is included if employees have questions. 2. e. Reviewed internal Human Resources documentation and noted that Sempra employees are required to protect and maintain the confidentiality of Customer Information. Disclosure of customer information is prohibited absent customer consent, for Primary Purposes, or pursuant to a legal process. 2. f. Reviewed internal Human Resources documentation and noted that no Sempra employee should access or otherwise use confidential customer information unless authorized to do so for legitimate business needs and in accordance with Company policies, laws, and regulations. 2. g. Reviewed internal Human Resources documentation and noted that non-public information, including Covered Information, may be used only for legitimate business purposes and unauthorized disclosure is prohibited. 2. h. Reviewed internal procedural documentation and noted there is a section on "Confidentiality and Privacy" which instructs employees that Covered Information shall only be accessed, used, and disclosed with a business need. The documentation contains information related to breach notification or if an employee has questions or concerns. All Branch Office employees must certify to department policies and procedures annually. 2. i. Reviewed internal privacy program documentation and noted that SDG&E instructs department employees on the definition of Primary and Secondary Purposes of Covered information; appropriate correspondence/authentication with customers; storage and disposal of Covered Information; the	

	proper methods for transferring information to Third Parties; and how to respond in the instance of Breach of Customer Privacy. 2. j. Reviewed the Call Center privacy program documentation and noted that it instructs Energy Service Specialists (ESS) on customer authentication and authorization for customer information disclosure to Third Parties. 2. k. Reviewed internal privacy program documentation and noted that it provides SDG&E employees with privacy tips to safeguard customer information while working remotely. 2. l. Met with Branch Office Supervisor, and was informed that all Branch Office ESS must certify annually to the Branch Office Policies and Procedures. 2. m. Met with the Supervisor, CCC Operations Support, and was informed that all CCC ESS must certify annually to CCC Policies and Procedures. Additionally, the Contact Center provides an intranet help website for ESS that includes department procedures and forms. 2. n. Reviewed the OCP intranet website and noted that it includes the following information for employees: ■ Privacy Definitions ■ Applicable Laws and Policies ■ Training and Awareness – Videos, FAQs, Tips ■ Privacy Tools ■ Breach Notification Requirements ■ Security Requirements ■ Help 2. o. Reviewed the Sempra Information Security intranet website and noted that it includes information for employees with access to the network regarding: ■ Policies & Procedures ■ Security Awareness and Education ■ Breach Notification Requirements ■ Security Alerts ■ Help 2. p. Reviewed internal privacy program documentation and noted that employees are required to annually certify to the proper safeguarding of Covered Information. 2. q. Reviewed the SDG&E Contact Center intranet website and noted that privacy materials were included:	

	■ Smart Grid Privacy Initiative ■ SDG&E Privacy Notice ■ Information Release for Imminent Threat ■ Third Party Data request 2. r. Reviewed internal CCC documentation and noted that ESS are required to annually certify to the workplace reminders which include proper safeguarding of Covered Information.	
3. Determine whether SDG&E tracks the categories of agents, contractors and other Third Parties to which they disclose Covered Information for a Primary Purpose.	3. a. Reviewed the SDG&E list of 245 Third Parties (Suppliers) with access to Covered Information in 2013. The list included Third Party name, SDG&E internal contact/contract owner and request status. The number of Third Parties matches those listed in *SDG&E's Annual Privacy Report*. 3. b. Reviewed a sample of SDG&E's Third Parties with access to Covered Information in 2013 and noted the description of each Supplier's location, type of work and need for access. 3. c. Met with Manager, Office of Customer Privacy, and was informed that the 245 Third Parties have an SDG&E employee identified as their sponsor who manages and oversees the contractual relationship. These employees are identified in the intranet system used by SDG&E for Third Party management.	
4. Determine whether SDG&E has secondary use authorization forms customers sign to authorize use of Covered Information for secondary uses.	4. a. Met with Manager, Office of Customer Privacy, and was informed that the company requires customer consent prior to disclosure of customer information for Secondary Purposes. The CISR form is the document used for customers to explicitly authorize the use of Covered Information for Secondary Purposes. 4. b. Reviewed the CISR form templates and a sample of executed CISR forms and noted the company has authorization forms for customers sign to authorize use of Covered Information for Secondary Purposes. 4. c. See CPUC Rule 6e (1)-(3) Audit Test Results 2. a – d.	
5. Determine whether a specific person or group within SDG&E is responsible or accountable for privacy and security policy development, implementation, monitoring, enforcing and updating.	5. a. Reviewed internal privacy program documentation and noted that the Privacy Program is led by the Chief Customer Privacy Officer and supported by a Director, the Office of Customer Privacy, and the SDG&E Privacy Steering Committee (SPSC). 5. b. Reviewed internal privacy program documentation and noted that it provides an overview and purpose of the SPSC and includes Membership roles, meeting frequency, and responsibilities. 5. c. Reviewed an internal audit report and noted that Audit Services performed a review of SDG&E's privacy processes including a Privacy Decision readiness assessment.	

	5. d. Met with Manager, Office of Customer Privacy, and was informed that the OCP supports all privacy initiatives for a) External Regulators, b) Customers, and c) SDG&E employees and provides tools to ensure that privacy is adequately addressed in new projects and system upgrades including the adoption of Privacy by Design and the use of a Privacy Impact Assessment tool. 5. e. Met with Vice President Customer Service/Chief Customer Privacy Officer, and was informed that the role includes: ■ Responsibility for the oversight of customer facing activities, including customer assisting programs and customer privacy. ■ Participation on an Executive Risk Committee that meets once per year and has Customer Privacy as its main focus. 5. f. Met with Director of Customer Programs, and was informed that the role oversees customer programs including Customer Privacy. The role is a part of the Executive Risk Directors Sub-Committee that analyzes risk and controls and escalates them as necessary to the Executive Risk Committee. 5. g. Met with Senior Vice President/Chief Information Officer, and was informed that the role oversees all IT activities for Sempra, including SDG&E and SoCalGas. The role is ultimately responsible for ensuring IS requirements are met. 5. h. Reviewed the job description for the Customer Programs Advisor and noted that the company sought a position reporting into the Manager, Office of Customer Privacy. Responsibilities include independent management, design, implementation and execution of various customer privacy processes. 5. i. Reviewed a sample of *SDG&E*'s *Privacy Steering Committee Meeting Minutes* from the period of review and noted that the Committee met in accordance with the requirements of the Charter. 5. j. Reviewed sample *PIAs* of projects performed in 2013 and noted that the assessments were completed in accordance with company policy. 5. k. Reviewed Management Corrective Actions prepared by Management and tracked by Audit Services in response to Business Control Issues identified in an audit report. Observed evidence that Audit Services tracked all Business Control Issues to closure.	
6. Understand the Compliance Area Leader's certifications/areas of expertise to determine qualification for responsibility and accountability of SDG&E's privacy program.	6. a. Met with Manager, Office of Customer Privacy and was informed that the role: ■ Serves an active member of the SDG&E privacy committee, which has regular meetings to discuss strategies for company's customer privacy matters and acts as an awareness channel for relevant groups. ■ Coordinates with Company's Attorney that monitors privacy legislation prior to or when a law is passed to discuss operational and customer impacts so business changes can be made to comply	

	with the new law. ■ Uses a variety of sources to track current privacy issues and topics, including subscriptions and external privacy related sources. ■ Holds the appropriate professional certifications. 6. b. Inspected public records identifying SDG&E's Privacy Compliance Program Leader (Manager, OCP) and his professional certifications.	

CPUC Rule 9	Rule Description	**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.
b		

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E provides notice to its customers on how they customers can contact the company for inquiries, complaints or disputes related to their personal information.	1. a. Reviewed the *Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information* and noted that it includes contact information for how a customer can contact SDG&E to complain, dispute, or inquire via Telephone, Email, and U.S. Mail. 1. b. Reviewed the SDG&E *Website Privacy Policy* and noted that it includes contact information for how a customer can contact SDG&E with questions or comments via Telephone, Email, and U.S. Mail.	
2. Determine whether SDG&E has a documented process to receive customer disputes, complaints, and inquiries, addresses and resolve complaints, and communicate resolution back to the customer in a timely and satisfactory manner.	2. a. Reviewed internal procedural documentation and noted that it describes that SDG&E has established a procedure for tracking complaints as required by the CPUC 2. b. Met with Supervisor, Customer Contact Centers (CCC) Operations Support and was informed that there are approximately 200 ESS across two SDG&E Contact Centers who interact directly with customers. ESS can interact via telephone, email, social media, and chat functions. 2. c. Met with Manager, CCC, and was informed that a process and resources exist to field complaints that are directed to the President or other SDG&E executives, arise from the CPUC, or are initiated through other channels including the Better Business Bureau, Elected Officials, or Consumer Advocacy groups. 2. d. Met with Manager, OCP, and was informed that the OCP has a direct email (OfficeofCustomerPrivacy@semprautilities.com) where customers can send inquiries and complaints.	
3. Determine whether SDG&E has a process to escalate disputes, complaints, and inquiries to help ensures resolution within a timely manner.	3. a. Reviewed internal procedural documentation and noted that a process exists to escalate customer complaints to a Supervisor or Associate Supervisor. 3. b. Met with Operations Support, CCC, and was informed that ESSs track customer complaints by type, source, and date of origin. 3. c. Reviewed internal procedural documentation and noted that complaints are tracked by sub-department and include complaint type and date of complaint origin and closure.	

4. Inspect evidence SDG&E tracks and resolves customer complaints consistent with SDG&E's policies.	4. a. Met with CCC Operations Support Analyst, and was informed that emails will be sent to those individuals who are assigned complaints to close complaints within 30 days of the date the complaint was opened. 4. b. Reviewed a sample customer complaint sent by a customer to the Office of Customer Privacy in March 2014 regarding the potential unauthorized disclosure of customer information to a Third Party. The complaint was resolved by the OCP over the course of three days and pursuant to the process described by management. 4. c. Reviewed internal complaint tracking records for the beginning of the Audit Period and noted that all complaints are tracked by sub-department for each month, quarter, and year-to-date. 4. d. Reviewed sample email communication from CCC Operations Support to an Associate Supervisor within the CCC who had been assigned a complaint. The reminder email informed the Associate Supervisor that all complaints should be resolved and closed within 30 days of the date the complaint was opened.	

CPUC Rule 9	Rule Description	**Training:** Covered entities shall provide reasonable training to all employees and contractors who use, store or process Covered Information.
c		

Audit Procedures	Audit Test Results	Exceptions
1. Review SDG&E's documented privacy awareness program materials to identify personnel who handle and access Covered Information.	1. a. Reviewed the list of the different business units within SDG&E that handle Covered Information, and noted each business unit is governed by operational-driven specific policies and procedures. In particular, the business units with access to Covered Information are the following: ■ Advanced Meter Operations ■ Billing Operations ■ CI Services ■ Credit and Collections ■ Customer Assistance – Low Income Programs ■ Customer Call Center ■ Demand Response ■ Home Area Network (HAN) Program ■ Load Research ■ Residential & Non-Residential EE 1. b. Met with Manager, OCP, and noted that there is a process for identifying business units with access to Covered Information, including a multi-step review of the different SDG&E business units to understand whether they have CEUD access. 1. c. Met with representatives from a sample of the business units with access to Covered Information and confirmed they are identified as groups with access to Covered Information. In addition, they confirmed they have been trained with regards to data privacy and are aware of the company privacy policies.	While company-wide Customer Privacy training was developed it was not consistently rolled out to cover new employees hired after the training was initially launched, or certain contractors with access to Covered Information.
2. Understand the awareness material and communications to SDG&E personnel to determine how internal privacy policies are communicated to associates.	2. a. Reviewed internal awareness documentation and noted that it provides all Sempra employees with resources to aid in maintaining Information Security. The following are included within the website: ■ *Quick Links* –Provides information regarding IS and announcements on upcoming company-wide privacy and IS events.	

	■ *Request* – Allows employees to manage their network access and provides guidance to remote and internet access to company records and information. ■ *Learn* – Contains information pertaining to the classification of data, methods for encrypting and protecting data transfer, password strengthening techniques, links to informational brochures informing employees of identity theft, as well as links to internal and external privacy and security websites. ■ *Report and Incident* –Allows employees to report instances of threats to privacy and data security. ■ *Policies & Procedures* – Lists internal information regarding the management and protection of sensitive information, guidelines for compliance with security policies, agreed standard company controls and security features, as well as detailed step-by-step instructions for information protection processes and activities. 2. b. Reviewed the SDG&E list of awareness programs and communications and noted that during the covered period there were multiple communication efforts to SDG&E personnel about customer privacy. These awareness materials and events include the following, among others: ■ An event for the utility employees for awareness related to privacy matters surrounding smart-grid customer information. ■ An event for internal employees for awareness on SDG&E customer privacy program, SDG&E customer privacy office and cyber security matters among others topics. ■ An invitation to an internal webinar about cybersecurity and privacy. ■ A web posting notifying employees about how to protect the company's information in social media. ■ News regarding potential risks of sharing CEUD. ■ A web posting informing employees about the updated privacy guidelines noting any additions. ■ A notice to employees about the new intranet site covering specific privacy matters and education materials. ■ Multiple articles related to the risks related to customer privacy, non-public information sharing and cyber-attacks. 2. c. Reviewed SDG&E internal OCP intranet website and noted multiple awareness and educational materials informing employees about the importance of customer privacy and data security. Some of the awareness materials include the following: ■ Informational page defining privacy and SDG&E's focus on customer privacy. ■ FAQs including topics for SDG&E employees to learn how to address privacy in day-to-day	

	operations. ■ Document repository for privacy related processes for departmental operations (e.g., PIAs). ■ Third Party information sharing specific website containing process overviews and documentation for employees to use when handling Third Party data requests. ■ List of SDG&E policies and procedures related to customer privacy and data security available (by link) to employees.	

3. Understand SDG&E's specific training materials to assess whether they adequately communicate/train employees on how to handle Covered Information. In addition, inspect that employees have completed these privacy and security training requirements.	3. a. Reviewed internal training documentation training and noted SDG&E communicates and trains employees on how to handle Covered Information. ■ This training is web-based for non-represented (non-unionized) employees and instructor led for represented (unionized) employees, with similar content in both cases. ■ The training content includes an interactive video with knowledge checks that discusses protecting Covered Information. ■ The web-based version includes a mandatory test and three certification questions for the employees to confirm that they have read and understood the Privacy Policy and they will comply with it. 3. b. Examined web-based training for new hires which includes knowledge checks, and which completion is tracked through an internal tracking system used by SDG&E for employee education. This training is targeted to non-represented employees and contains the following modules: ■ A training module providing education regarding protecting confidential entity related information such as financial records, company assets, records management, and regulatory compliance. ■ A training module addressing non-public information sharing among SDG&E's internal departments and it also addresses general privacy and information protection. ■ A training module addressing information disclosures between affiliated entities and the necessary customer consent, including when related to CEUD. ■ A training module including information regarding rules and regulations governing retention periods for documentation, and address general privacy and information protection. 3. c. Reviewed New Employee Orientation Documentation and noted that it references trainings and customer privacy related content that the employee will need to take and consider for their work. 3. d. Met with Billing Operations Support, Senior Service Advisor and with Advisor, Regulatory Compliance and noted that while company-wide Customer Privacy training was developed it was not consistently rolled out to cover new employees hired after the training was initially launched, or certain contractors with access to Covered Information. In addition, we noted that SDG&E plans to launch a formal training for contractors. 3. e. Reviewed sample training logs for web-based privacy training targeted for non-represented employees and noted that training requirements are tracked for this group of employees. 3. f. Reviewed sample training logs for instructor-led privacy training targeted for represented employees and noted the training has not been consistently rolled out for this group of employees 3. g. Met with Advisor, Regulatory Compliance and learned about the training required for union employees and the corresponding tracking controls in place. It was also stated that HR is functionally responsible for this training.	

4. Inspect evidence that contractors have completed privacy and security training requirements (e.g., training logs, certifications of compliance, etc.).	4. a. Reviewed internal privacy training materials for contractors and noted SDG&E had designed the content of this training to be provided to contractors in the future which includes requirements for handling Covered Information. 4. b. Met with Advisor, Regulatory Compliance to discuss the specific training materials given to the entity's contractors and were informed that: ■ Employee Contractors (contractors on SDG&E direct payroll) receive the web-based SDG&E training, similar to non-represented employees. ■ Contractors engaged by the utility through a temporary workforce solution company are not required to take the SDG&E privacy training; however information privacy requirements are noted in the language within the contract and signed NDA agreements. ■ The upcoming training for SDG&E contractors will be rolled out during the second half of 2014.	
5. Understand the privacy training required of Third Parties accessing Covered Information in order to determine whether or not they are adequately equipped to handle Covered Information.	5. a. Met with Manager, OCP, and understood that vendors are contractually obligated per their contract clauses to maintain the privacy of the information shared. SDG&E does not independently deliver trainings, provide training materials, or validate whether these training took place for Third Party vendors. 5. b. Met with Advisor, Regulatory Compliance and was informed that SDG&E does not independently deliver trainings, provide training materials, or validate whether these training took place for Third Party vendors. SDG&E relies on the contractual relationship between itself and Third Parties to ensure that Third Parties train their own internal resources on proper data handling techniques. 5. c. Inspected 24 SDG&E Contract Templates used by supply management for Third Party contracting and noted that the 24 documents contain a clause covering the: ■ *Prohibition on Non-Public Information Sharing* stating that the contractor will agree not to disclose or allow access to any non-public information and that contractor may be required to complete training at Sempra's discretion. ■ *Confidentiality* indicating that the contractor agrees to use the Confidential Information solely for the purpose of performing services under the agreement. 5. d. Reviewed *SDG&E Non-Disclosure Agreement* templates and noted that they include a section entitled "*Limited Use –Nondisclosure"*: ■ *The Mutual Non-Disclosure Agreement* states that neither party nor its representatives shall use the confidential information of the other party for its own benefit ■ *The One-Way Non-Disclosure Agreement* states that neither the Third Party nor its representatives shall use the confidential information for their own benefit	

	5. e. Met with Portfolio Manager, IT/Telecommunications to discuss the contract templates currently in use with Third Parties. Confirmed that non-disclosure and privacy language is enforced, and that only in exceptional cases contractual terms and conditions are modified from those originally included in the templates. 5. f. Inspected an executed Third Party contract sample and noted that it includes the prohibition on Non-Public Information Sharing clause and the Confidentiality clause.	

CPUC Rule 9	Rule Description	Reporting Requirements:
e		On an annual basis, each electrical/gas corporation 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.

Audit Procedures	Audit Test Results	Exceptions
1. Determine whether SDG&E tracks the reporting requirement and assigns compliance to the appropriate department(s).	1. a. Met with Manager, Office of Customer Privacy and was informed that the OCP is responsible for collecting the information to complete the *CPUC Annual Privacy Report*. The OCP uses a report template which contains a table of all the report's requirements and step-by-step instructions for the appropriate stakeholders to collect the data elements. Additionally, the OCP Manager will email the Directors at the beginning of each year to remind them of their responsibility to provide information. 1. b. Reviewed Privacy Decision compliance tracking documentation and noted that a section within provides the stakeholder name and the source of the data to be included in the *Annual Privacy Report*. 1. c. Reviewed sample email from Manager, OCP sent to all Directors and VP Direct Reports instructing them to provide information that would be included in the *Annual Privacy Report*.	
2. Determine whether SDG&E filed its Annual Report to the CPUC as required by the Privacy Decision.	2. Reviewed the *SDG&E 2013 Annual Privacy Report* and noted that it was submitted to the CPUC on April 30, 2014 by Director, Regulatory Affairs. The report indicated: ■ 245 authorized Third Parties accessing Covered Information from SDG&E during 2013 (includes suppliers, contractors, vendors under contract with IOU, customer-authorized researchers or governmental requests, and customer-authorized Third Parties) and ■ Zero (0) instances of non-compliances with the *Privacy Rules* or with contractual provisions required by the *Privacy Rules* which become known to SDG&E through its daily operations during 2013 and that the number of customers impacted was not applicable.	