Company: Southern California Gas Company (U 904 G) / San Diego Gas & Electric Company (U 902 M)
Proceeding: 2024 General Rate Case
Application: A.22-05-___
Exhibit: SCG-41/ SDG&E-46

PREPARED DIRECT TESTIMONY OF

LAUREN GODINEZ FRAZER

(COMPLIANCE)

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

May 2022

TABLE OF CONTENTS

APPENDICES

SUMMARY

- My testimony presents the compliance-related items primarily associated with Southern California Gas Company's (SoCalGas) and San Diego Gas & Electric Company's (SDG&E) Test Year (TY) 2019 General Rate Case (GRC) Decision (D.) 19-09-051.
- This testimony also describes SoCalGas's and SDG&E's compliance with requirements from California Public Utilities Commission (CPUC or Commission) directives derived from other proceedings since the last GRC.

PREPARED DIRECT TESTIMONY OF LAUREN GODINEZ FRAZER (COMPLIANCE)

I. INTRODUCTION

A. Summary of Proposals

My testimony presents the status of SoCalGas's and SDG&E's compliance with Commission directives. Most of the compliance items discussed herein are associated with compliance items ordered in D.19-09-051, SoCalGas's and SDG&E's TY 2019 GRC Decision. D.19-09-051 was approved by the Commission on September 26, 2019 (*i.e.*, the effective date) and was issued on October 1, 2019 (*i.e.*, the issuance date).

Of all the potential SoCalGas and SDG&E compliance action items identified, only those that impact this general rate case are addressed in this exhibit.

To derive the list of compliance items provided in my testimony, I reviewed D.19-09-051 and other Commission directives and reporting requirements. This testimony is a product of my research.

B. Organization of Testimony

My testimony is organized in four sections as follows:

I. Introduction

II. Requirements in D.19-09-051 Included in the TY 2024 GRC

III. Other Compliance Items and Reporting Requirements Beyond D.19-09-051

IV. Witness Qualifications

II. REQUIREMENTS IN D.19-09-051 INCLUDED IN THE TEST YEAR 2024 GRC

Table LGF-1 below provides an overview of the compliance items from D.19-09-051 and the status of each. For each compliance action item, the following information is provided:

- Compliance Item: This usually consists of a quote of the applicable language from the decision. In general, if the decision citation includes an Ordering Paragraph, the "Compliance Item" will only quote such Ordering Paragraph. In some instances, other decision language will be quoted to help clarify the compliance item.

- Decision Reference: This indicates where the identified compliance action may be found in the Commission decision or resolution. The Decision Reference may refer to any combination of Ordering Paragraph or Discussion pages.
- Status: A status of "Complete" is provided for items that have been addressed in this GRC filing. Otherwise, a brief explanation is provided.

TABLE LGF-1

Compliance Item	**Decision Reference**	**Status**
Application [17-10-007/008 are] granted to the extent set forth in [D.19-09-051]. SoCalGas and SDG&E are authorized collect, through rates and through authorized ratemaking accounting mechanisms, the 2019 test year base revenue requirement, effective January 1, 2019.	Ordering Paragraphs 1 & 2	Complete, on-going for post-test years
Within 30 days from the effective date of this Order, Southern California Gas Company (SoCalGas) and San Diego Gas & Electric Company (SDG&E) shall each shall file respective Tier 1 Advice Letters with revised tariff sheets to implement the revenue requirements authorized in Ordering Paragraphs 1 and 2. a. The revised tariff sheets shall become effective on January 1, 2019 subject to a finding of compliance by the Commission's Energy Division, and compliance with General Order 96-B. b. The balances recorded in SoCalGas' and SDG&E's respective General Rate Case Revenue Requirement Memorandum Accounts from January 1, 2019 until the effective date of the new tariffs required by this Ordering Paragraph shall be amortized in rates thirty days after the effective date of this decision through December 31, 2021."	Ordering Paragraph 3	Complete
SoCalGas and SDG&E are each authorized to implement a Post-Test Year Ratemaking mechanism for 2020 and 2021, as follows: a. Labor and non-labor costs as well as medical costs be based on the IHS (Information Handling Services) Markit Global Insight forecast; b. Capital investments be based on an escalated seven-year average of capital additions and for	Ordering Paragraph 4	Complete

Compliance Item	Decision Reference	Status
SoCalGas, a forecast of Pipeline Safety Enhancement Plan capital additions beyond Test Year 2019; and c. Continuation of their currently authorized Z-Factor mechanisms.		
SoCalGas and SDG&E shall update their Post-Test Year revenue requirements by filing respective Tier 1 advice letters two months prior to the beginning of each attrition year. To adjust the revenue requirement for 2020, SoCalGas and SDG&E shall each file a Tier 1 Advice Letter with the Commission's Energy Division on or before November 1, 2019 with the update to the Test Year 2019 revenue requirement to be effective on January 1, 2020. Similarly, Tier 1 Advice Letters are to be filed on November 1, 2020 to adjust the revenue requirement for 2021 beginning on January 1, 2021.	Ordering Paragraph 5	Complete
Beginning in Post-Test Year (PTY) 2020, SDG&E shall adjust its PTY revenue requirements to reflect the equity rate base exclusion required by Assembly Bill 1054. SDG&E shall file a Tier 3 Advice Letter concurrent with its year-end adjustment filing for 2019, providing a detailed explanation and showing of the revenue requirement impact of the Public Utilities Code section 8386.3(e) equity rate base exclusion when it makes its annual PTY revenue requirement implementation filings.	Ordering Paragraph 6	Complete

Compliance Item	Decision Reference	Status
SoCalGas regulatory account proposals are authorized except as follows: a. Fire Hazard Prevention Memorandum Account (FHPMA). Recovery of balances under the FHPMA is authorized subject to a reduction of $0.1 million representing interest as SoCalGas should have sought recovery of this balance at an earlier time; b. Discontinuation of Service Establishment Charges (SEC). SoCalGas's request to eliminate the SEC is denied; c. Pipeline Safety Enhancement Plan Balancing Account (PSEPBA). Authority to establish the PSEPBA is denied. SoCalGas is instead authorized to establish a Pipeline Safety Enhancement Plan (PSEP) memorandum account to track PSEP costs and request recovery of amounts in excess of the amounts authorized in this decision; d. Morongo Rights-of-Way Balancing Account (MROWBA). Authority to establish the MROWBA is denied. Costs proposed to be recorded in the MROWBA must instead be tracked in the Morongo Rights-of-Way Memorandum Account; e. Liability Insurance Premium Balancing Account (LIPBA). SoCalGas shall file a Tier 2 advice letter when it seeks recovery of costs for additional liability insurance coverage that were not requested in this General Rate Case; and f. SoCalGas shall be allowed to include capital compounding calculations to its capital expenses for its Transmission Integrity Management Program (TIMP), Distribution Management Integrity Program (DIMP) and Storage Integrity Management Program (SIMP) Balancing Accounts.	Ordering Paragraph 7	Complete

Compliance Item	Decision Reference	Status
SDG&E's regulatory account proposals are authorized except as follows: a. FHPMA. Recovery of balances under the FHPMA is authorized subject to a reduction of $44,712 representing interest as SDG&E should have sought recovery of this balance at an earlier time; b. Tree Trimming Balancing Account (TTBA). Modification of the TTBA from a one-way to a two-way balancing account is authorized. However, SDG&E is required to file a Tier 3 Advice Letter for recovery of undercollections up to 35 percent and an application for undercollections above 35 percent; c. LIPBA. SDG&E shall file a Tier 2 advice letter when it seeks recovery of costs for additional liability insurance coverage that were not requested in this General Rate Case; and d. SDG&E shall be allowed to include capital compounding calculations to its capital expenses for its TIMP and DIMP Balancing Accounts.	Ordering Paragraph 8	Complete
SoCalGas and SDG&E shall comply with Resolution E-4963 and track in their respective Officer Compensation Memorandum Accounts officer compensation and benefits that are still included in their respective Test Year 2019 revenue requirements.	Ordering Paragraph 9	Complete
SoCalGas and SDG&E shall track officer salaries, bonuses, and benefits in cost centers that are embedded with other costs in their respective Officer Compensation Memorandum Accounts.	Ordering Paragraph 10	Complete
"The Officer Compensation Memorandum Account balances shall be trued-up in Southern California Gas Company’s and San Diego Gas & Electric Company’s respective year-end adjustment filings for 2019 and the amounts refunded to ratepayers."	Ordering Paragraph 11	Complete
Officer salaries, bonuses, and benefits shall be excluded from the revenue requirements for Post-Test Years 2020 and 2021.	Ordering Paragraph 12	Complete

Compliance Item	Decision Reference	Status
SoCalGas shall file a Tier 2 Advice Letter at the conclusion of Line 235 West Sections 1 and 2 testing or replacement with clear accounting delineations of which costs are subject to the TIMP and which costs are subject to the Pipeline Safety Enhancement Plan (PSEP) before any associated Line 235 PSEP pressure testing costs can be placed into rates for recovery. Such PSEP costs shall not be placed into rates for recovery and such TIMP costs shall be made subject to refund until the Advice Letter is approved. The Line 235 costs subject to this accounting requirement include costs SoCalGas is incurring for the additional permits, crews, environmental monitoring, and all other costs associated with investigating and repairing the ongoing leaks on Line 235. Line 235 repair costs in TIMP will be reviewed in a future general rate case.	Ordering Paragraph 13	The ordering paragraph directs SoCalGas to file an advice letter at the conclusion of Line 235 West Sections 1 and 2 testing or replacement. The conclusion of testing or replacement has not occurred.
SoCalGas shall establish a memorandum account within 20 days from the effective date of this decision and at that time shall begin to record all costs related to Line 235 West Sections 1 and 2 (*i.e.*, capital costs including rate of return, operations and maintenance costs, repair and replacement costs, or any other costs related to the line).	Ordering Paragraph 14	Complete
To ensure that pipelines under Phase 2b comply with D.11-06-017, SoCalGas shall file the re-testing implementation plan as part of SoCalGas's 2019 Risk Assessment Mitigation Phase (RAMP) filing, and the plan shall specifically include the following: a. Identification of all in-service natural gas transmission pipelines (by location and including linear feet and the pipelines' categorization in Class locations 1-4) that were tested under the ASA Code and for which test records exist; b. Identification of the subset of the above qualifying pipelines for which SoCalGas recommends and does not recommend a re-test, in particular in Class 1 locations in areas that are not High Consequence Areas, and a statement explaining why a re-test is proposed or not proposed; c. Presentation of the pre-1970 ASA Code test records for the pipelines proposed to be re-	Ordering Paragraph 15	Complete

Compliance Item	Decision Reference	Status
tested, and direct comparison of the test elements shown in the records to the test elements set out in 49 CFR 192.619; d. An evaluation by an independent engineer that SoCalGas's proposed determination of which pipelines to re-test or not to re-test is a reasonable engineering judgement; e. The forecast costs of re-testing; and f. Consistent with the RAMP framework, a complete discussion of the risk-spend efficiency of the dollars proposed to be spent.		
SoCalGas shall file a Tier 2 Advice Letter to request project substitution of an approved PSEP with another project. The advice letter will contain the name and scope of the delayed project, the circumstances that led to the substitution, and identification of the substituted project as well as the scope and estimated costs to complete the substituted project.	Ordering Paragraph 16	Complete
SDG&E shall file a Tier 1 Advice Letter to establish a one-way balancing account for Overhead Pools within 60 days from the effective date of this decision.	Ordering Paragraph 17	Complete
Southern California Gas Company and San Diego Gas & Electric Company shall update their respective uncollectible expense rate for Post-Test Years 2020 and 2021 by filing respective annual Tier 1 Advice Letters to the Commission's Energy Division.	Ordering Paragraph 18	Complete
Within 180 days from the effective date of this decision, SoCalGas shall file a Tier 3 Advice Letter certifying that it is dedicating the additional funding of $0.859 million for Customer Services Field & Meter Reading to improving its reconnection rates and explain, with specificity, what steps it is taking to ensure that reconnection times stay within that 36-hour period. The Advice Letter must demonstrate that SoCalGas is complying with the 36-hour reconnection period without underfunding or understaffing other work and shall also provide information about customer wait times for safety concerns and service requests and show that those wait times are reasonable for customers requesting assistance in English as well as in other languages.	Ordering Paragraph 19	Complete

Compliance Item	Decision Reference	Status
SDG&E shall file a Tier 2 Advice Letter to request recovery of reasonable costs in excess of the authorized amount for third-party claims.	Ordering Paragraph 20	Complete
SoCalGas and SDG&E shall file separate Tier 2 Advice Letters to seek appropriate adjustment to its revenue requirement for any difference between including and excluding cost of removal from the Average Rate Assumption Method (ARAM) calculation in the event that the Internal Revenue Service (IRS) issues formal guidance contrary to the approach this decision takes in disallowing exclusion of costs of removal from the ARAM calculation.	Ordering Paragraph 21	In May 2022, the IRS ruled that the Commission's method for computing ARAM (*i.e.*, including cost of removal in the calculation) was inconsistent with the tax normalization rules, while the SoCalGas/SDG&E method for computing ARAM (*i.e.*, excluding cost of removal) was consistent with the tax normalization rules. Therefore, SoCalGas and SDG&E will file separate Tier 2 Advice Letters to seek appropriate adjustment to the revenue requirement.
The decision also incorporates 2019 impacts from the Tax Cuts and Jobs Act (TCJA) and directs SDG&E and SoCalGas to file separate Advice Letters with the Commission's Energy Division to begin the process of returning to ratepayers 2018 tax savings from the TCJA.	Ordering Paragraph 22	Complete
SDG&E shall remove costs for two projects concerning the Palomar plant that should have been disallowed in 2012 but were still included in the revenue requirement beginning in 2016.	Ordering Paragraph 23	Complete
In its next GRC filing, SoCalGas shall include testimony confirming any costs associated with Morongo Rights-of-Way negotiations and resolution of negotiations if an agreement is reached.	Ordering Paragraph 25	Complete
SoCalGas shall include a Safety Management Systems	Ordering	Complete

Compliance Item	Decision Reference	Status
proposal in its next GRC application.	Paragraph 26	
In its next GRC, SoCalGas shall include an outlook of its long-term assessment and replacement plan for Aldyl-A pipes and bare steel pipes without cathodic protection, in addition to assessment and replacement activities planned for the next GRC cycle.	Ordering Paragraph 27	Complete
SDG&E shall include an outlook of its long-term assessment and replacement plan of its Aldyl-A pipes and the Distribution Risk Evaluation and Monitoring System program pipe replacement in its next GRC in addition to the activities planned for the next GRC cycle.	Ordering Paragraph 28	Complete
San Diego Gas & Electric Company shall submit a report in its next General Rate Case detailing actual project costs for the Advanced Energy Storage (AES) project. The report shall include the specific costs of procuring the energy storage systems and a summary of the specific benefits realized by ratepayers.	Ordering Paragraph 29	Complete
SoCalGas shall host an annual workshop during the second quarter of 2020 and 2021 under supervision of the Commission's Energy Division. At these workshops, SoCalGas shall present the result of the previous year's Research, Development, and Demonstration (RD&D) program and obtain input regarding its intended spending for the following calendar year. Prior to the workshop, SoCalGas shall: a. Submit a report to Energy Division staff describing prior years' RD&D program including a summary of ongoing and completed projects; funds expended, funding recipients, and leveraged funding; and an explanation of the process used for selecting RD&D project areas as well as the structure of SoCalGas' RD&D portfolio; b. Provide Energy Division staff with the workshop presentation materials as well as documentation of stakeholders consulted in the development of RD&D projects, both at least one week before the workshop; and c. Engage relevant stakeholders to encourage their attendance at the workshop, such as the California Energy Commission, Gas Technology Institute, the U.S. Department of Energy, and other organizations engaged in gas research and development. SoCalGas must also present its budget broken down by research projects, request for proposals, and funding amounts. Other specific details	Ordering Paragraph 30	Complete

Compliance Item	Decision Reference	Status
concerning the workshops must be coordinated with the Commission's Energy Division staff.		
SoCalGas and SDG&E shall provide testimony in their next General Rate Cases on the current funding levels and outstanding balance of their Pension Benefit Obligations so the Commission can assess whether any modifications are needed.	Ordering Paragraph 31	Complete
In their next respective GRC applications, SoCalGas and SDG&E must include a report in the form of testimony that details the studies conducted, findings made, and steps taken regarding a multi-method framework to assess safety culture and including contractors in safety culture assessments.	Ordering Paragraph 32	Complete
If a decision adopting a four-year General Rate Case cycle is made in Rulemaking 13-11-006, Southern California Gas Company and San Diego Gas & Electric Company shall file a petition for modification of this decision to request review and implementation of Southern California Gas Company's and San Diego Gas & Electric Company's post-test year proposals for 2022.	Ordering Paragraph 33	Complete
Regarding CUE's proposal for an additional replacement of 25 regulators, we find that this premature at this time. However, we agree with CUE that SoCalGas should develop some sort of ranking system for regulator replacements. SoCalGas should include this information in its next GRC and should use this ranking system as part of the basis for determining its proposed regulator replacement rate in its next GRC.	Section 7.1.3.17., p. 63	Complete
Continuation of the Aliso Canyon Memorandum Account (ACMA) to record additional capital-related costs in excess of $275.5 million authorized for the Aliso Turbine Replacement project should be authorized subject to a reasonableness review of any additional	Section 14.3, p. 173-174	Complete

Compliance Item	Decision Reference	Status
costs in SoCalGas' next GRC.		

III. OTHER COMPLIANCE ITEMS AND REPORTING REQUIREMENTS BEYOND D.19-09-051

Table LGF-2 below provides an overview of the compliance requirements from Commission directives pertaining to other proceedings since the last GRC and new legislation and the status of each. For each compliance action item, the following information is provided:

- CPUC Decision or Public Utilities Code that resulted in the compliance action item.
- Compliance Item: This usually consists of a quote of the applicable language from the decision. In general, if the decision cite includes an Ordering Paragraph, the "Compliance Item" will only quote such Ordering Paragraph. In some instances, other decision language will be quoted to help clarify the compliance item.
- Reference: This indicates where in the Commission decision or resolution the identified compliance action may be found. The Decision Reference may refer to any combination of Ordering Paragraph or Discussion pages.
- Status: A status of "Complete" is provided for items that have been addressed in this GRC filing. Otherwise, a brief explanation is provided.

TABLE LGF-2

Compliance Item	Reference	Status
D.21-05-003 (SoCalGas's and SDG&E's PTY Mechanism for 2022 and 2023)		
Within 30 days from the effective date of this Order, SoCalGas and SDG&E shall each file respective Tier 2 advice letters to implement the revenue requirement modifications to Decision (D.) 19-09-051 specified in Ordering Paragraph (OP) 1a to 1u of D.20-07-038. The modifications shall be effective as of January 1, 2019. However, OP 1j and 1k are hereby corrected such that the total amount of promotional gear for SoCalGas is $134,000 and for SDG&E $64,000.	Ordering Paragraph 3	Complete

SoCalGas shall update its post-test year revenue requirements for 2022 and 2023 by filing Tier 1 advice letters with the Commission's Energy Division two months prior to the beginning of each post-test year. To adjust the revenue requirement for 2022, SoCalGas shall file a Tier 1 advice letter on or before November 1, 2021 to update its revenue requirement for January 1, 2022 through December 31, 2022. Similarly, SoCalGas shall file a Tier 1 advice letter on or before November 1, 2022 to update its revenue requirement for January 1, 2023 through December 31, 2023.	Ordering Paragraph 6	Complete for 2022 Post-test year
To adjust the revenue requirement for 2022, SDG&E shall file a Tier 1 advice letter with the Commission's Energy Division on or before November 1, 2021 to update its revenue requirement for January 1, 2022 through December 31, 2022. Similarly, SDG&E shall file a Tier 1 advice letter on or before November 1, 2022 to update its revenue requirement for January 1, 2023 through December 31, 2023.	Ordering Paragraph 7	Complete for 2022 Post-test year
Within 45 days from the date of this Order, SDG&E shall file a Tier 2 advice letter with the Commission's Energy Division to implement Resolution E-5069 which approved Advice Letter 3352-E. The Resolution removes from the 2019 GRC revenue requirement adopted in D.19-09-051 costs tracked in the Rate Reform Memorandum Account relating to Marketing, Education and Outreach activities for the 2019 Default Time of Use. SDG&E shall also propose necessary adjustments to the authorized revenue requirements for all attrition years included in the 2019 GRC cycle.	Ordering Paragraph 8	Complete
California Public Utilities Code Section 8386.4		
The commission shall consider whether the cost of implementing each electrical corporation's plan is just and reasonable in its GRC. Each electrical corporation shall establish a memorandum account to track costs incurred for fire risk mitigation that are not otherwise covered in the	Pub. Util. Code § 8386.4(b)(1)	Complete

electrical corporation's revenue requirements. The commission shall review the costs in the memorandum accounts and disallow recovery of those costs the commission deems unreasonable.		
The chief executive officer of an electrical corporation shall certify in each general rate case application that the electrical corporation has not received authorization from the commission to recover the costs in a previous proceeding, including wildfire cost recovery applications.	Pub. Util. Code § 8386.4(b)(3)	Complete; Certification attached to this GRC Application
Compliance with D.18-12-014 (the Safety Model Assessment Proceeding [S-MAP] Decision) and Ruling Directing Sempra Utilities to Incorporate Staff Recommendations on their RAMP in the 2024 GRC		See the testimony of Gregory S. Flores and R. Scott Pearson (RAMP to GRC Integration) (Ex. SCG-03/SDG&E-03, Chapter 2)
D.18-05-022 (Establishing Reentry Fees and Financial Security Requirements for Community Choice Aggregators)		
Accordingly, the utilities are directed to file a Tier 1 Advice Letter that provides a detailed description of the specific services that are covered, their corresponding costs, and how those costs were calculated.	Ordering Paragraph 3	Complete
In their next general rate case, each utility must identify the administrative fee as a separate item, describe its components and how it is calculated, and provide a comparison of its fee with that of the other major California utilities.	Ordering Paragraph 4	Complete
Resolution E-5030		
SDG&E must cease booking costs into the Distributed Generation Statistics Memorandum Account (DGSMA) after the effective date of the rates established by its next GRC.	Ordering Paragraph 1	Complete
SDG&E, beginning in its next GRC, may recover costs for work performed by the contractor for the California Distributed Generation Statistics website through its GRCs.	Ordering Paragraph 3	Complete
D.19-08-002 (SoCalGas to Incorporate Advanced Metering Infrastructure Data into its Scheduling and Balancing Process)		

Applicants shall file a Tier 1 Advice Letter to establish a Memorandum Account in which Applicants may record costs of the Advanced Metering Infrastructure Data Aggregation System, automation of Scheduled Quantity trading for ENVOY, and other costs associated with requiring Gas Acquisition to balance to estimated actual consumption, for consideration in the next General Rate Case.	Ordering Paragraph 8	Complete

D.18-08-008 (Granting Authority to Implement Customer Information System (CIS) Replacement)		
In each of SDG&E's future general rate cases, SDG&E will present an updated forecast of the total benefit amount broken down into the 45 distinct benefits identified by SDG&E.	Settlement Agreement Provision 2.2	Complete
D.20-06-003 (Accepting Changes to Reduce CA Resident Disconnections)		
Fee based revenue that was collected via reconnection fees may be addressed in SoCalGas's and SDG&E's next general rate case and incorporated into base rates.	Ordering Paragraph 17	Complete
Any costs associated with the Arrearage Management Plan (AMP) should be addressed in the utilities next GRC.	Section 15.5.2, p. 109	Complete
D.18-06-028 (Re: Certificate of Convenience and Necessity for the Pipeline Safety & Reliability Project)		
Within one month of the date of the issuance of this decision, SoCalGas and SDG&E shall file a Tier 1 Advice Letter requesting a memorandum account to record costs associated with the audit of the Line 1600 records (to be reviewed for reasonableness and amortization in its next GRC or applicable formal proceeding.)	Ordering Paragraph 12, and p. 100	Complete
Assemby Bill (AB) 802		
Pursuant to Section 5 of AB 802, SoCalGas established the AB802 Memorandum Account in order to record incremental costs related to the implementation of AB 802. The disposition of the account balance and cost recovery mechanism for the AB802MA will be addressed in SoCalGas' next General Rate Case proceeding or other applicable proceeding.	Section 5	Complete
D.16-06-007 (Update Portions of the Commission's Current Cost-Effectiveness Framework)		
The utility is authorized to seek recovery of costs booked to this memorandum account in a general rate case proceeding and should demonstrate that the costs are reasonable and incremental to current revenue requirements.	Ordering Paragraph 8	Complete
D.21-06-013 (Revising Electric Rule 20)		

Each utility must track actual expenditures and seek cost-recovery periodically through the General Rate Case applications.	p. 28	Complete
D.18-03-023 (Track 3 Policy Issues, Sub-Track 2 (Grid Modernization))		
We direct the IOUs to add grid sensors and remote controlled switches in the classification tables. If the IOUs find that changes to the classification system are necessary to more accurately reflect their GRC proposals, they may propose modifications via Tier 2 Advice Letter, with sufficient time to make adjustments to the GRC filing, in the event of a resolution. Parties may recommend alternate modifications to the classification tables in their protests to the advice letter.	Ordering Paragraph 3	Complete
The investor-owned utilities (IOUs), in their GRC filings on grid modernization, shall use the tools developed in the Distribution Resources Plan proceeding to present the level of distributed energy resource penetration system integration challenges that are expected to arise on the grid, and what the most cost-effective mitigation options or investments are.	Ordering Paragraph 4	Complete
The investor-owned utilities (IOUs) shall identify the drivers of grid needs in the Grid Needs Assessment and propose the most appropriate method to quantify the Distributed Energy Resources integration costs to incorporate into the Locational Net Benefit Analysis. The IOUs shall file their Grid Modernization Plan as a chapter in their GRC.	Ordering Paragraph 7	Complete
D.21-06-015 (Approval of Energy Savings Assistance and California Alternate Rates for Energy Programs)		
The utility cooling centers must be funded through the respective utility's general rate case, since cooling centers benefit all patrons, and not just low income patrons.	Ordering Paragraph 19	Complete
D.21-10-019 (Track 2 Pole Owner Databases)		
For pole owners subject to a GRC, those costs incurred to implement the decisions in this proceeding shall be distributed as appropriate between electric utility rates for electric attachments (*e.g.,* cost of cataloging and making available in the pole database for any attachment	Ordering Paragraph 24	Complete

data), and for pole attachment rates for costs incurred for communications attachments (*e.g.*, cost of managing data submissions from attachers, providing technical support staff, information technology equipment).		
D.11-07-056 & D.12-08-045 (Privacy Decisions)		
Audit of Data Privacy and Security Practices	Ordering Paragraphs 4 and 5	Complete; See Appendices B & C

This concludes my prepared direct testimony.

IV. WITNESS QUALIFICATIONS

My name is Lauren Godinez Frazer. My business address is 555 West Fifth Street, Los Angeles, California 90013. I am currently a Regulatory Case Manager in the GRC and Revenue Requirements department within the Regulatory Affairs organization representing both Southern California Gas Company and San Diego Gas & Electric Company. I have held this position since July of 2017.

I have a bachelor's degree in Economics from San Diego State University, Cum Laude. I started my employment with Sempra Energy in 2011. I have held various positions of increasing responsibility in the departments of Compliance, Procurement, Supply Management, and Advanced Metering Infrastructure -Project Management Office before assuming a position in Regulatory Affairs.

In my current role, I manage regulatory proceedings including the Risk Assessment Mitigation Phase, and aspects of the Test Year 2024 General Rate Case. In addition, I supervise the Regulatory Case Support group, which serves as central files for SoCalGas and SDG&E and processes regulatory-related information requests.

I have not previously testified before the Commission.

APPENDIX A

Glossary of Terms

APPENDIX A

Glossary of Terms

AES:	Advanced Energy Storage
ACMA:	Aliso Canyon Memorandum Account
A.:	Application
ARAM:	Average Rate Assumption Method
AB:	Assembly Bill
AL:	Advice Letter
ALJ:	Administrative Law Judge
AMP:	Arrearage Management Plan
CIS:	Customer Information System
CPUC:	California Public Utilities Commission
CUE:	Coalition of California Utility Employees
D.:	Decision
DGSMA:	Distributed Generation Statistics Memorandum Account
DIMP	Distribution Management Integrity Program
FHPMA:	Fire Hazard Prevention Memorandum Account
GRC:	General Rate Case
ICP:	Incentive Compensation Plan
IHS:	Information Handling Services
IOUs:	Inverstor-Owned Utilities
IRS:	Internal Revenue Service
LIPBA:	Liability Insurance Premium Balancing Account
MROWBA:	Morongo Rights-of-Way Balancing Account
OP:	Ordering Paragraph
PSEPBA:	Pipeline Safety Enhancement Plan Balancing Account
PTY:	Post-Test Year
R.:	Rulemaking
RAMP:	Risk Assessment Mitigation Phase
RD&D:	Research, Development and Demonstration
SB:	Senate Bill
SDG&E:	San Diego Gas & Electric Company
SEC:	Service Establishment Charges
SIMP:	Storage Integrity Management Program
SoCalGas:	Southern California Gas Company
TCJA	Tax Cuts and Jobs Act
TIMP:	Transmission Integrity Management Program
TTBA:	Tree Trimming Balancing Account
TY:	Test Year

APPENDIX B

SoCalGas Covered Information Privacy and Security Assessment Report

Southern California Gas Company

CPUC Covered Information Privacy and Security Assessment Report

For the period January 1, 2021
through December 31, 2021

February 25, 2022

kpmg.com

Contents

Document structure

This report consists of the following sections:

Executive summary – an overview of the project including background, scope, and KPMG's overall results and noted exceptions and recommendations, where necessary, for each Rule comprising the *California Public Utility Commission Privacy Decision*.

Project approach and methodology – an overview of key project phases and activities performed by KPMG throughout the course of the assessment.

Rule assessment results, exceptions, and recommendations – a summary of KPMG's assessment associated with each of the nine (9) Rules of the *CPUC Privacy Decision* including KPMG's interviews and document reviews (e.g., test work), overall results, detailed exceptions, and improvement recommendations associated with each exception.

SoCalGas' Management Response to CPUC Covered Information Privacy and Security Assessment Report – SoCalGas' Management Response to the *CPUC Covered Information Privacy and Security Assessment Report* dated February 23, 2022.

Appendix I – Detailed assessment procedures and results – the full details of KPMG's assessment criteria, procedures, and results for each Rule.

Appendix II – Abbreviations used in this report – a list of the abbreviations and acronyms used throughout this Report.

Appendix III – Stakeholders interviewed – a list of stakeholders interviewed by KPMG throughout the course of the assessment.

Executive summary

Through its Advanced Meter and meter-to-cash operations, Southern California Gas Co. (hereinafter "SoCalGas," the "Utility." or "Company") collects, processes, stores, and discloses Customer Energy Usage Data (CEUD) and other Customer Personally Identifiable Information (PII). The PII contains names, addresses, Social Security Numbers, service account numbers, and financial account information. When combined, CEUD and PII represent Covered Information.

Background

On August 23, 2012, the California Public Utilities Commission (CPUC) issued 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" (hereinafter the "*Privacy Decision*"). The *Privacy Decision* requires SoCalGas to undergo an independent assessment of its Covered Information privacy and security practices. Covered Information is defined in the *Privacy Decision* as CEUD obtained via Advanced Metering Infrastructure combined with other information that could reasonably be used to identify a residential customer, family, household, residence, or nonresidential customer. Covered Information does not include information provided to the CPUC pursuant to its oversight responsibilities.

SoCalGas engaged KPMG to conduct an independent assessment of the Company's Covered Information privacy and security processes, controls, and practices in conjunction with general rate case proceedings.[1] This report represents the results of KPMG's assessment.

Prior to the period under review, the US Department of Health and Human Services declared a national health emergency due to the COVID-19 pandemic. As a result, the State of California declared a State of Emergency and executed a stay-at-home order causing the majority of SoCalGas' workforce to migrate to a remote working environment. SoCalGas adapted and adjusted several of its safeguards and processes over Covered Information in light of the new remote working environment impacting the vast majority of the workforce. This remote working environment remained in effect during the covered period (2021); KPMG's team also adjusted its approach to deliver the assessment by using various forms of media, technology, and a virtual team infrastructure to execute this assessment 100% remotely.

[1] Independent privacy and security practices assessment is not intended to be an audit, examination, attestation, special report or agreed-upon procedures engagement as those services are defined in American Institute of Certified Public Accountants literature applicable to such engagements. Accordingly, these services will not result in the issuance of a written communication to third parties by KPMG directly reporting on financial data or internal control or expressing a conclusion, an opinion, or any other form of assurance.

Scope

The scope of KPMG's assessment was limited to systems and Lines of Business (LOBs) collecting, processing, storing, or disclosing Covered Information. The scope does not cover an assessment of SoCalGas' practices, procedures, and controls to safeguard employee or contractor PII, or other customer PII that is not Covered Information.

To perform the review, KPMG used an Assessment Framework comprised of multiple criteria based on various industry leading standards. KPMG mapped the Assessment Framework criteria to the nine (9) Rules in the *Privacy Decision* and used the framework to perform the assessment of SoCalGas' privacy and security practices, procedures, and controls to safeguard Covered Information.

— The *Covered Information Privacy and Security Practices Assessment* was based on KPMG's review and understanding of the practices, procedures, and controls in place from **January 1, 2021 through December 31, 2021** (the Covered Period).

— The exceptions and recommendations were based on KPMG's review of policy/procedure documents, stakeholder interviews, inspection of sample communications to customers and third parties, Covered Information access reports, system security profiles, and virtual site walk-throughs.

— In typical years, KPMG would perform physical site walk-throughs to observe physical, technical, and administrative privacy and security controls implemented where Covered Information is collected, stored, and processed. However, as a result of the global pandemic, KPMG was unable to conduct physical site walk-throughs as part of the 2021 assessment. KPMG did conduct virtual site walk-throughs of a Contact Center, Billing and Processing Center, Sempra Production Data Center, and two Branch Offices. KPMG's observations are limited to observations identified through such virtual site walk-throughs, stakeholder interviews, virtual screen sharing and documentation reviews.

— KPMG conducted 36 interviews with personnel from various LOBs including Customer Operations, Customer Services, Audit Services, Cybersecurity Risk & Compliance, Systems & Technology, Customer Contact Centers, Digital Enablement Services, Litigation, Support Services, Corporate Security, Security Compliance & Executive Services, Cloud & Infrastructure, Technology & Business Services, Enterprise Risk & Compliance, Digital & Consumer, General Counsel- Regulatory, CPUC/ FERC- Gas, Policy & Proceedings, Supply Management & Div Business, Digital Workspace & Automation, and Remittance Processing. KPMG also conducted interviews with SoCalGas privacy and security executives to understand general Covered Information oversight, management, and tone at the top.

— KPMG assessed the design and implementation of privacy and security controls, followed by an assessment of operating effectiveness of key implemented controls.

The nine (9) Rules noted in the *Privacy Decision* 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

Summary of exceptions

KPMG has noted **3** Exceptions (Exceptions are areas where SoCalGas' program may not be fully prepared to meet compliance with CPUC *Privacy Decision* requirements, as measured against KPMG's Assessment Framework, developed to test controls around Covered Information identified in the rules). The Exceptions are shown below along with the recommendations associated with each Exception. There were **2** Low-Risk Exceptions, **1** Medium-Risk Exception, and **0** High-Risk Exceptions.

The risk rating methodology is based on the following definitions:

Risk level	Description
High	Issue poses a significant risk of data breach of Covered Information and/or a significant deviation from the *CPUC Privacy Decision*.
Medium	Inconsistent implementation of policies and procedures that may impact the ability of SoCalGas to protect Covered Information and/or achieve adequate alignment with the *CPUC Privacy Decision*.
Low	Procedures or practices supporting the protection of Covered Information and alignment with the *CPUC Privacy Decision* may not be formally defined or documented.

For more details associated with each Rule, see **Rule assessment results, exceptions, and recommendations,** and **Appendix I – Detailed assessment procedures and results**.

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	**Low**	SoCalGas' *Privacy Notice* provided to customers states that the customer may contact SoCalGas if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.	Management should consider updating SoCalGas' *Privacy Notice* to include the consequences a customer may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.
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**	Sampled SoCalGas contracts executed since the completion of the prior	Management should consider performing a risk assessment of the legacy third party contracts

		Covered Information assessment and current standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, while one of the sampled vendor contracts executed prior to the effective date of the Privacy Decision and amended in 2014 contains confidentiality language, KPMG observed privacy and security provisions that do not align to formal regulatory requirements.	governing the sharing of Covered Information with third parties. The risk assessment should consist of a variety of factors, including the date of contract execution/renewal, the privacy and security terms of the contract, the sensitivity of Covered Information provided to the third party, the volume of customer records, and the results of the most recent third-party security assessment. For contracts determined to be higher risk where the privacy and security terms of the contract are not aligned with the Privacy Decision requirements, Management should consider renegotiating the contracts to include the required language to help ensure Covered Information and customer privacy protections are properly managed by the third parties in alignment with the Privacy Decision. Note: In this context, "legacy contracts" are considered active agreements with third parties involving the sharing of Covered Information dated prior to SoCalGas' implementation of current standard contract template.
CPUC Rule 7 Data Quality and Integrity	-	-	N/A
CPUC Rule 8 Data Security	-	-	N/A
CPUC Rule 9 Accountability and Auditing	**Low**	SoCalGas has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their onboarding. This will help to ensure contractors are properly trained in a timely

		engaged after the training was initially launched.	manner on how to access, collect, store, use, and disclose Covered Information.

Project approach and methodology

KPMG approached the Assessment in four (4) main phases: Mobilize, Assess, Validate, and Report.

— **Mobilize –** KPMG validated the Assessment Framework used to review SoCalGas's privacy and security practices based on the nine (9) Rules comprising the *Privacy Decision*. KPMG created this framework at the inception of the *Privacy Decision*, and it has been used across all the California IOUs. The framework has evolved overtime to reflect changes in the environment, market expectations and Utilities maturing programs.

  KPMG worked with SoCalGas' Privacy team to identify relevant stakeholders, reviewed the organizational structure to identify business groups where Covered Information may reside, reviewed the current IT landscape to identify systems and applications that collect, store, or process Covered Information, and documented existing system profiles for systems and applications that collect, store and process Covered Information.

— **Assess –** As part of this assessment, KPMG performed a variety of interviews with stakeholders representing various LOBs. KPMG interviewed a unique total number of **72** personnel in a total of **36** interviews, submitted **198** document requests, reviewed approximately **360** documents and **20** system assessments, and performed **5** virtual site walk-throughs of critical SoCalGas facilities (Customer Contact Center, Data Center, Credit and Billing Center, and two Branch Offices) to observe safeguards in place to protect Covered Information.

— **Validate –** KPMG validated draft observations throughout the Assessment phases with the SoCalGas Privacy team, relevant IT and business stakeholders, and SoCalGas leadership.

— **Report –** KPMG developed a final report providing exceptions and recommendations and incorporated SoCalGas' Management Response to the validated Exceptions.

Rule assessment results, exceptions, and recommendations

For each identified Exception, KPMG reviewed the risk and assigned a risk rating of **High, Medium,** or **Low** based on the potential impact the Exception could have as it relates to the protection of Covered Information. The risk rating methodology used the following definitions:

Risk level	Description
High	Issue poses a significant risk of data breach of Covered Information and/or a significant deviation from the *CPUC Privacy Decision*.
Medium	Inconsistent implementation of policies and procedures that may impact the ability of SoCalGas to protect Covered Information and/or achieve adequate alignment with the *CPUC Privacy Decision*.
Low	Procedures or practices supporting the protection of Covered Information and alignment with the *CPUC Privacy Decision* are not formally defined or documented.

KPMG noted **3** specific Exceptions, comprised of **2** Low-Risk Exceptions, **1** Medium-Risk Exception, and **0** High-Risk Exceptions. The Exceptions identify areas where SoCalGas' program is not fully prepared to meet requirements under the *Privacy Decision*.

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

Rule 2: Transparency Notice

KPMG assessment procedures	KPMG assessed SoCalGas' overall customer notice program focusing on: — Review internal and customer-facing *Privacy Policies* and *Privacy Notice* that address SoCalGas' practices and procedures related to the collection, processing, storage, and disclosure of Covered Information; — Interview SoCalGas Privacy Team personnel and review of methods and frequency for providing customers with the *Privacy Notice*; — Interview Customer Service Specialists (CSSs) to discuss interactions with customers and discussing their Covered Information.
Results summary	SoCalGas provides its external-facing *Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information* (*Privacy Notice*) and *Privacy Policy* 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 a contact telephone number and mailing address where customers can contact SoCalGas with complaints, inquiries, and disputes regarding their Covered Information and SoCalGas' *Privacy Notice*. There is a "Privacy" link located at the bottom of SoCalGas' homepage, which takes the customer to privacy related resources, including the *Privacy Notice*. SoCalGas provides its *Privacy Notice* to new customers upon registration, and annually thereafter in a bill insert. The *Privacy Notice* is available in 13 languages to accommodate SoCalGas' largest customer demographics. SoCalGas also makes available its previous versions of the *Privacy Notice* upon request. Customers can email webmaster@socalgas.com or contact the Contact Center to request prior versions of SoCalGas' *Privacy Notice*.
Exception	No Exceptions noted
Risk level	-
Risk implication	-
Recommendation	-

Rule 3: Purpose Specification

KPMG assessment procedures	KPMG assessed SoCalGas' specification of the purposes focusing on: — Review how SoCalGas specifies the reasons for which it collects, discloses, retains, and provides access to Covered Information; — Review of SoCalGas' *Privacy Notice*, as well as other policies and procedures; — Interview stakeholders to understand the determination and specification of information and third-party categories; — Examine whether the *Privacy Notice* includes a description of how customers can access and control their Covered Information collected, processed, stored, and disclosed by SoCalGas; — Interview SoCalGas personnel on procedures to assist customers with accessing, inquire about, or dispute their covered information.
Results summary	SoCalGas has documented policies and procedures outlining the acceptable purposes for which Covered Information may be collected, stored, used, and shared. These include detailed policies regarding disclosure of Covered Information for both primary and secondary purposes. In addition, the *Privacy Notice* includes ways the Customer can contact SoCalGas to limit the collection, use, and storage of Covered Information. Per Company policy, Covered Information is not disclosed for secondary purposes, without customer authorization. SoCalGas' *Privacy Notice* includes the categories of third parties with which SoCalGas may share Covered Information, and circumstances under which that information may be shared. SoCalGas has implemented internal policies, procedures, and standards instructing employees on determining the veracity and propriety of third-party requests for customer information, the relevant customer consent forms, and on the appropriate use of Covered Information.
Exception	SoCalGas' *Privacy Notice* provided to customers states that the customer may contact SoCalGas if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.
Risk level	**Low**
Risk implication	Per CPUC *Privacy Decision*, customers must be informed of the consequences associated with limiting their Covered Information in order to be able to make informed decisions related to their information.
Recommendation	Management should consider updating SoCalGas' *Privacy Notice* to include the consequences a customer may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.

Rule 4: Individual Participation (Access and Choice)

KPMG assessment procedures	KPMG assessed SoCalGas' customer-facing program focusing on: — Review internal and external policies and procedures to provide customers with access and consent mechanisms related to their Covered Information; — Review customer portals, perform stakeholder interviews, and conduct virtual walk-throughs of the Customer Contact Center and Branch Offices where SoCalGas CSSs interact with customers with respect to their Covered Information; — Review customer authorization forms to understand how customers can grant and revoke authorization of their Covered Information for secondary purposes; — Examine 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 SoCalGas stakeholders in relevant business functions.
Results summary	SoCalGas provides customers with multiple methods to access their Covered Information, including on their monthly bills, via SoCalGas' *MyAccount* portal and *Home Energy Reports* that allow them to review and interpret their CEUD. Customers may contact SoCalGas through phone, web, email, or mail with questions or concerns regarding their Covered Information, account, and monthly bills. SoCalGas CSSs authenticate customers and validate their account information when answering calls prior to addressing customers' questions or concerns. Internal guidelines for SoCalGas employees who interact with customers are in place and address how to provide customers with access to their Covered Information. SoCalGas has processes and procedures in place for customers to grant and revoke authorization to third parties through the use of the *Customer Information Service Request (CISR)* form. Customer-facing policies and notices indicate SoCalGas may disclose Covered Information if it is necessary to provide energy services, to comply with relevant laws, to respond to subpoenas or warrants, or to provide emergency responders with pertinent information in the case of imminent threat to life or property. While the *2021 Annual Privacy Report* is not available as of the date of this report, KPMG had access to and reviewed SoCalGas' *2020 Annual Privacy Report* and noted SoCalGas received nine demands to disclose Covered Information pursuant to legal process and zero requests for Covered Information due to imminent threat to life or property.
Exception	No Exceptions noted
Risk level	-
Risk implication	-
Recommendation	-

Rule 5: Data Minimization

KPMG assessment procedures	KPMG assessed SoCalGas' adoption of Data Minimization principles in the collection, use, and disclosure of Covered Information focusing on: — Review corporate and department-specific policies and procedures to understand how Covered Information is segregated from other systems; — Interview stakeholders to determine how user access to Covered Information is limited based on business need; — Examine how records and assets are retained for only as long as reasonably necessary; — Inspect the proper disposal of records upon their eligibility for disposition; — Interview stakeholders to determine how Data Minimization principles were adopted as part of third-party disclosure practices; — Perform virtual site walk-throughs at the Customer Contact Center, Branch Offices, and interviews with CSSs to understand how Data Minimization is implemented in the Contact Centers, Branch Offices, and in a remote working environment.
Results summary	SoCalGas has implemented the Data Minimization principle as a foundational component to its overall privacy program framework. The company has documented policies and procedures limiting the amount of information collected, stored, and retained; the number and level of employees who have access to Covered Information; and the categories of third parties with whom it is shared. SoCalGas enforces the same Data Minimization protocols within the Contact Centers and Branch Offices as they do for employees working remotely. Data Minimization is reinforced through various trainings and employee compliance with relevant policies and procedures is routinely reviewed. SoCalGas management reviews and certifies that Covered Information is retained only as long as necessary for a specific business purpose and that it is properly disposed of in a timely manner.
Exception	No Exceptions noted.
Risk level	-
Risk implication	-
Recommendation	-

Rule 6: Use and Disclosure Limitation

KPMG assessment procedures	KPMG assessed SoCalGas' Third-Party Management Program focusing on: — Examine processes in place for disclosure of Covered Information to third parties. "Third party" is defined to include suppliers and contractors; — Review procedures and forms for customers to authorize and revoke a third party to receive Covered Information on behalf of the customer; — Examine third-party management policies and procedures and interview of stakeholders to understand how SoCalGas implements practices and procedures based on the categories of third parties; — Review third-party contract management processes including onboarding, contract compliance reviews, and contract termination; — Review third-party (suppliers, vendors, contractors and consultants) risk management documentation; — Examine data transmission protocols and ongoing monitoring of third parties for compliance with SoCalGas policies and contractual provisions.
Results summary	SoCalGas has processes in place to allow customers to share their Covered Information with third parties. SoCalGas has formal internal procedures to manage customer requests for disclosure to third parties, which include forms for explicit customer authorization and forms to revoke such authorization (CISR forms). Prior to providing services to SoCalGas, all third parties must have a written formal agreement and must undergo a risk assessment conducted by the Information Technology Vendor Management Office (IT VMO). In addition, SoCalGas has internal third-party management policies and informs third parties about data privacy requirements. Third-party vendors are contractually obligated to maintain the privacy of the information shared.
Exception	Sampled SoCalGas contracts executed since the completion of the prior Covered Information assessment and current standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, while one of the sampled vendor contracts executed prior to the effective date of the Privacy Decision and amended in 2014 contains confidentiality language, KPMG observed privacy and security provisions that do not align to formal regulatory requirements.
Risk level	**Medium**
Risk implication	Third-party vendors with access to Covered Information may have safeguards to protect customer privacy at levels less protective than those under which SoCalGas operates.
Recommendation	Management should consider performing a risk assessment of the legacy third party contracts governing the sharing of Covered Information with third parties. The risk assessment should consist of a variety of factors, including the date of contract execution/renewal, the privacy and security terms of the contract, the sensitivity of Covered Information provided to the third party, the volume of customer records, and the results of the most recent third-party security assessment. For contracts determined to be higher risk where the privacy and security terms of the contract are not aligned with the Privacy Decision requirements, Management

	should consider renegotiating the contracts to include the required language to help ensure Covered Information and customer privacy protections are properly managed by the third parties in alignment with the Privacy Decision. Note: In this context, "legacy contracts" are considered active agreements with third parties involving the sharing of Covered Information dated prior to SoCalGas' implementation of current standard contract template.

Rule 7: Data Quality and Integrity

KPMG assessment procedures	KPMG assessed SoCalGas' data validation methods and procedures focusing on: — Interview stakeholders to determine how SoCalGas validates the quality and integrity of Covered Information; — Examine the Advanced Meter systems and infrastructure to understand how usage data is managed and reconciled; — Review policies and procedures and interviews with stakeholders to understand how SoCalGas provides customers with the opportunity to modify or remove other data elements collected by the Company.
Results summary	SoCalGas has policies in place that address the confirmation, validation, and relevance of customer information. The *Privacy Notice* provides customers with details to contact the Company by phone, email or mail should they need to view or dispute their information. In addition, Contact Center personnel authenticate and validate customer account information when answering a call. CSSs can assist customers with updating their information. SoCalGas' *MyAccount Terms and Conditions* indicate it is the customers' responsibility to ensure their personal information is updated and accurate. System checks and manual processes are in place to validate energy usage reads and perform edits to help 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 assessment procedures	KPMG assessed SoCalGas' physical and Cybersecurity measures to protect Covered Information focusing on: — Review Cybersecurity policies, procedures, and measures related to: endpoint security (antivirus protection, email/database security), network security (network segmentation, Intrusion Prevention Systems/Intrusion Detection Systems, remote access, wireless, firewalls, network access controls), logging and monitoring, data loss prevention, web-content filtering, mobile security, vulnerability and patch management, business continuity/disaster recovery, change control (SDLC, cybersecurity assessments, privacy impact assessments, secure code reviews), access management (user provisioning and deprovisioning, access governance, privileged access, third-party access), and data classification; — Perform virtual site walk-throughs to observe and validate the physical and technical security controls implemented to safeguard Covered Information at the following critical SoCalGas facilities: Customer Contact Center, a Branch Office, Production Data Center, Credit Operations and Billing Operations; — Inspect system profiles for in-scope systems storing Covered Information related to key configurations and system settings: System Access (user authentication and password configuration), Access Management (restriction of access based on least privilege and need-to-know, segregation of duties, periodic access reviews), Logging and Monitoring (system activity reviews, audit logs and audit trails of changes to customer data), Disaster Recovery, Data Protection (secure transfer mechanisms, encryption, masking of sensitive data); — Review the Sempra and SoCalGas incident response and breach management program and interview stakeholders who are responsible and/or accountable in the response to a potential incident involving Covered Information, including communications to regulators and impacted customers; — Review evidence of tools deployed in the environment to detect and analyze potential threats to Covered Information.
Results summary	SoCalGas has a well-established Information Security (IS) Program as part of Sempra shared services that is responsible for the design and implementation of both physical and logical information security controls to protect Covered Information. Formal policies and procedures have been established and implemented that address specific administrative, physical, and technical controls to protect Covered Information. Monitoring procedures are in place to detect and address noncompliance with policies and procedures. Various technical controls have been implemented to prevent and detect incidents and unauthorized access to systems containing Covered Information. A process is also in place to report and track potential security incidents and breaches to help ensure they are contained and eradicated, and measures are implemented to reduce the likelihood of similar events from occurring in the future.
Exception	No Exceptions noted.
Risk level	-
Risk implication	-

Recommendation	-

Rule 9: Accountability and Auditing

KPMG assessment procedures	KPMG assessed SoCalGas' overall Customer Data Privacy and Cybersecurity programs, focusing on: — Review documentation supporting each program as well as SoCalGas' communication of these policies to both employees and contractors; — Interview stakeholders to understand the level of executive support and sponsorship of the Customer Privacy Program and Cybersecurity program, including the individuals and roles responsible and accountable for the customer privacy and cybersecurity throughout the Company; — Interview members of SoCalGas Executive Management to understand leadership's views on customer data protection; — Review processes to receive, track and resolve customer complaints, disputes, and inquiries related to the protection of Covered Information. Test procedures included a review of internal procedures, interviews with stakeholders involved in the complaints process, and virtual walk-throughs of the Customer Contact Center and Branch Offices; — Examine the employee and contractor training and awareness programs associated with the protection of Covered Information. This assessment included a review of enterprise-wide and targeted training materials provided to SoCalGas employees and third-party contractors collecting, handling, storing, or transmitting Covered Information. Additionally, KPMG observed training compliance logs maintained for privacy trainings for employees and contractors.
Results summary	SoCalGas has developed Company and department policies addressing proper safeguards of Covered Information. The Company has achieved a high level of maturity for its Customer Privacy Program, including a dedicated Customer Privacy Program Officer and Manager, which provides executive and management support, oversight, and visibility to reporting. Updates on data privacy and cybersecurity are regularly provided to management and the Board of Directors, and the Company's officers and directors reinforce the importance through awareness programs and town halls. A process exists to respond to complaints and inquiries levied by customers related to customer privacy. A Company-wide cybersecurity training and privacy training has been implemented and a targeted Customer Data Privacy Training is provided to employees and contractors that have access to Covered Information.
Exception	SoCalGas has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.
Risk level	**Low**
Risk implication	Contractors on-boarded after the annual launch of the training could use, process, or store Covered Information without being trained on how to handle Covered

	Information. In addition, a contractor could start and end their work assignment without being required to complete Covered Information training.
Recommendation	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their onboarding. This will help to ensure contractors are properly trained in a timely manner on how to access, collect, store, use, and disclose Covered Information.

SoCalGas Management Response to CPUC Covered Information Privacy and Security Assessment Report

February 23, 2022

Doron Rotman
Managing Director
KPMG LLP

Re: Southern California Gas Company's Response to KPMG's 2021 Covered Information Privacy and Security Assessment Report

Dear Mr. Rotman:

On behalf of Southern California Gas Company ("SoCalGas") we would like to thank you for the professional services KPMG provided in performing the 2021 SoCalGas Covered Information Privacy and Security Assessment.

SoCalGas engaged KPMG to perform this independent assessment to validate our company's compliance as required in the California Public Utilities Commission (CPUC) 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*. We appreciate that KPMG recognizes that SoCalGas is in compliance with most of the rules in D.12-08-045 and that SoCalGas is continuing to strengthen its Customer Privacy Program.

SoCalGas reviewed the exceptions contained in KPMG's 2021 Covered Information Privacy and Security Assessment Report and provides the following attached response.

Sincerely,

Janet M. Yee

Janet M. Yee
Director, Customer Operations

Attachment

CPUC rule number	Risk level	Exceptions noted	KPMG recommendations	SCG Management Response
CPUC Rule 1 Definitions	-	-	N/A	
CPUC Rule 2 Transparency (Notice)	-	-	N/A	
CPUC Rule 3 Purpose Specification	**Low**	SoCalGas' Privacy Notice provided to customers states that the customer may contact SoCalGas if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.	Management should consider updating SoCalGas' *Privacy Notice* to include the consequences a customer may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.	Because limiting collection, use, storage, or disclosure of Covered Information is not an applicable concept under the regulatory requirements, consequences of limiting are also not an applicable concept. Instead, the applicable concept is consent. SCG must obtain a customer's consent for secondary purposes. SCG will make it more clear in our privacy notice when consent is required.
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**	Sampled SoCalGas contracts executed since the completion of the prior Covered Information assessment and current standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, while one of the sampled vendor contracts executed prior to the effective date of the Privacy	Management should consider performing a risk assessment of the legacy third party contracts governing the sharing of Covered Information with third parties. The risk assessment should consist of a variety of factors, including the date of contract execution/renewal, the privacy and security terms of the contract, the sensitivity of Covered Information provided to	SCG includes required contract language when Covered Information is involved. Supply Management works with business, legal, and vendors to ensure that the appropriate language is included in contract templates that involve Covered Information. The specific language in SCG templates is sometimes subject to

		Decision and amended in 2014 contains confidentiality language, KPMG observed privacy and security provisions that do not align to formal regulatory requirements.	the third party, the volume of customer records, and the results of the most recent third-party security assessment. For contracts determined to be higher risk where the privacy and security terms of the contract are not aligned with the Privacy Decision requirements, Management should consider renegotiating the contracts to include the required language to help ensure Covered Information and customer privacy protections are properly managed by the third parties in alignment with the Privacy Decision. Note: In this context, "legacy contracts" are considered active agreements with third parties involving the sharing of Covered Information dated prior to SoCalGas' implementation of current standard contract template.	negotiations between SCG and vendors. However, in those circumstances where language is negotiated, it still requires in totality a level of protection consistent with the regulatory requirements.
CPUC Rule 7 Data Quality and Integrity	-	-	N/A	
CPUC Rule 8 Data Security	-	-	N/A	
CPUC Rule 9 Accountability and Auditing	**Low**	SoCalGas has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their onboarding.	SCG will assign the required Covered Information contractor training on a more timely basis, at the time that they are onboarded, instead of the

		consistently rolled out to contractors engaged after the training was initially launched.	This will help to ensure contractors are properly trained in a timely manner on how to access, collect, store, use, and disclose Covered Information.	current annual process of offering this training.

Appendix I - Detailed assessment procedures and results

CPUC RULE 2 – Transparency (Notice)

Overall assessment result		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has documented policies addressing the provision of notice to customers of SoCalGas' data collection and handling techniques.	1.a. Reviewed SoCalGas' *Tariff Rule 42 Privacy and Security Protections for Energy Usage Data* and noted it provides guidance to SoCalGas employees regarding: — how to use and protect CEUD, — how the notice is provided to customers, and what it must include, — how customers can control their energy usage data, and — how SoCalGas must only collect, store, use, or disclose as much CEUD as necessary or authorized by the CPUC to meet specific operational or business needs. 1.b. Reviewed the *Customer Privacy Program Standard Operating Procedures* and noted SoCalGas' Privacy Program is based on the Generally Accepted Privacy Principles (GAPP) which helps organizations design and implement comprehensive privacy programs. This document also addresses SoCalGas program members' responsibilities and mentions how "SoCalGas desires to work collaboratively with external partners to find ways to advance [their] customer privacy program and only share customer data within the terms of the *Privacy Notice*." 1.c. Viewed links to the *Privacy Notice* and *Privacy Policy* on SoCalGas' website. SoCalGas' *Privacy Notice* informs customers why SoCalGas collects energy usage information, how long SoCalGas retains their energy usage information, when SoCalGas shares energy usage information, how to view their energy usage information online, and how to view *Privacy Notices* online. The *Privacy Notice* mentions "[SoCalGas] will update this *Notice* as necessary and will inform customers of the update by posting the revised *Notice* on our website. We will also notify you annually to visit the most updated version of this *Notice*." 1.d. Visited Company website and noted the homepage contains a link to the privacy center where privacy-related links are attached, including: *Privacy Policy*, *Privacy Notice*, and a link for the *Privacy Policy* and *Privacy Notice* in additional languages. 1.e. Met with SoCalGas' Privacy Team and noted there are three mechanisms used to share the *Privacy Notice*: — A copy sent to customers upon registration,	

Assessment procedures	Assessment test results	Exceptions
	— A billing insert sent every year, and — SoCalGas' website. 1.f. Met with members of the Privacy Team and was informed the *Privacy Notice* is reviewed annually and no updates have been made since 2014. If changes to the *Privacy Notice* are made, customers are informed with a billing insert and the *Privacy Notice* on the website is updated.	
2. Assess whether a procedure exists to assess whether new customers receive notice of the Company's privacy policy upon registration and annually thereafter.	2.a. Met with members of SoCalGas' Privacy Program and learned customers receive the *Privacy Notice* upon registration and annually. The *Privacy Notice* is also publicly available on the SoCalGas website. 2.b. Met with members of the Privacy Team and was informed when customers first register, they receive the *Start Service Request Confirmation* email, as well as the *Notice to New Customers* email. 2.c. Reviewed the *Start Service Request Confirmation* email and noted it contains links to the SoCalGas *Privacy Policy* and *Privacy Notice*. Also reviewed the *Notice to New Customers* email and noted it contains the SoCalGas *Privacy Notice*. 2.d. Reviewed the October *Privacy Notice* annual bill insert and noted it contains a copy of the *Privacy Notice* and SoCalGas' *Privacy Policy* web address. This insert also includes contact information where customers can request a current or prior version of the *Privacy Policy* and obtain answers to any privacy questions, concerns, or complaints.	
3. Assess whether SoCalGas provides notice to customers on an annual basis and when signing up new customers as required by the CPUC regulation.	3.a. Reviewed the *Notice to New Customers* email, sent to new customers when confirming a new account, and noted it contains a written version of the SoCalGas *Privacy Notice*. Also reviewed the *Start Service Request Confirmation* email, a second email sent when confirming a new customer account, and noted this electronic correspondence to new customers includes a link to the *Notice*. 3.b. Reviewed the October *Privacy Notice* annual bill insert and noted it contains a copy of the *Privacy Notice*, the web address of SoCalGas' *Privacy Policy*, and contact information to request a copy of the current or prior policy and to obtain answers to questions, concerns, or complaints.	

Assessment procedures	Assessment test results	Exceptions
	3.c. Visited SoCalGas' public website and noted a section for "Billing Inserts and Other Notices", including documents provided to customers from 1/1/2021 to 12/31/2021. The billing inserts within this section included copies of the SoCalGas *Privacy Notice* provided to customers with their bill in each month of the covered period. See site here: https://www.socalgas.com/regulatory/bill-inserts?__cf_chl_managed_tk__=pmd_JdVDdggG7aw7tfkZm0ommZo1W2.ukBot0L.MgyJAvwg-1634154946-0-gqNtZGzNAyWjcnBszQk9 3.d. See CPUC Rule 2b(2) for Test Results.	

CPUC Rule 2 c(1)-(2)	Rule description	**When provided:** 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.

Assessment procedures	Assessment test results	Exceptions
1. Review SoCalGas' methods for providing customers notice about their privacy and accessing the *Privacy Notice*.	1.a. See CPUC Rule 2b for Test Results. 1.b. Visited SoCalGas' website and noted the word "Privacy" at the bottom of the homepage; clicking on it brings the user to the SoCalGas Privacy Center, which houses all privacy-related links, including links to the *Privacy Policy* and *Privacy Notice*. 1.c. Met with members of SoCalGas' Privacy Program and learned customers receive a copy of the Company's *Privacy Notice* upon registration and annually.	
2. Assess 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. Reviewed SoCalGas' *Privacy Notice* and noted customers can provide feedback regarding the *Privacy Notice*. 2.b. SoCalGas' *Privacy Notice,* available online and provided as monthly billing inserts, includes normal font sizes, appropriate spacing, and it does not seem longer than necessary to convey the requisite information.	
3. Assess whether SoCalGas' *Privacy Notice* is written in an easy-to-understand language.	3.a. Performed a Flesch-Kincaid reading level test on the *Privacy Policy* and noted it was written at a college-level Flesch-Kincaid reading level (16th grade). 3.b. Performed a Flesch-Kincaid reading level test on the *Privacy Notice* and noted it was written at a college-level Flesch-Kincaid reading level (15th grade). 3.c. Noted the *Privacy Policy* and *Privacy Notice* are available in English, Spanish, Arabic, Armenian, Chinese, Farsi, Hmong, Khmer, Korean, Russian, Tagalog, Thai, and Vietnamese. Contact information is available to customers for comments, questions, or concerns regarding the *Privacy Policy* and *Privacy Notice*.	

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

Assessment procedures	Assessment test results	Exceptions
1. Understand the procedures in place to identify covered entities and assess whether the effective date is indicated in the relevant documentation.	1.a. Reviewed the *Privacy Notice* and noted it identifies SoCalGas as the covered entity and states July 2014 as the effective date. 1.b. Reviewed SoCalGas' *Privacy Notice* available online and noted a section informing customers how to access past and current *Privacy Notices*. Customers may call 1-800-427-2200 (Residential Customers), 1-800-427-2000 (Business Customers), mail their request to the address provided for the Customer Privacy Program Manager, or email webmaster@socalgas.com. 1.c. Reviewed SoCalGas' *Tariff Rule 42 Privacy and Security Protections for Energy Usage Data*, and noted the document identifies a 'covered entity' as: — SoCalGas or any third party that provides services to SoCalGas under contract, — Any third party who accesses, collects, stores, uses, or discloses Covered Information pursuant to an order of the Commission, unless specifically exempted, who obtains this information from SoCalGas, or — Any third party, when authorized by the customer, that accesses, collects, stores, uses, or discloses Covered Information relating to 11 or more customers who obtains this information from SoCalGas.	
2. Understand how the regulatory requirements, management review and approval process	2.a. Met with members of the Privacy Team and noted SoCalGas has not made any changes to the *Privacy Notice* since 2014. Although there is not a formally documented procedure, if a change was made, SoCalGas' Privacy Team would send the proposed changes to the Legal, Internal	

Assessment procedures	Assessment test results	Exceptions
works, including potential alterations of the privacy policies.	Communications, and Web Teams for approval before implementation. Once finalized, the Internal Publication Team (an extension of the Communication Group) would print and send out the updated notices. 2.b. Met with members of the Privacy Team and noted there is an informal annual process to review the SoCalGas *Privacy Notice*. On an annual basis, the Communications Team inquires the Privacy Team for any changes that may need to be made to the *Privacy Notice*. The Privacy Program Manager works with the Communications Team for any changes, and a final review is performed by a different member of the Privacy Team (responsible for the Privacy Program and Customer Operations). Any updates made are sent to the Web Team to update the website accordingly. Any substantive changes to the *Privacy Notice* are reviewed by Sempra's Legal Department. This review of the *Privacy Notice* is documented through emails. 2.c. Reviewed *SoCalGas Customer Privacy Program: Compliance Plan* and noted that as of September 29, 2021, the task: "Prepare and publish *Privacy Notice* (regarding energy usage)" showed 100% completion. This document also noted "*Notice* drafted, reviewed and posted on SCG's external website", as well as "Initially posted Online in December 2012 at http://www.socalgas.com/privacy-notice.shtml; Reviewed annually by Privacy Team. No major updates since inception." 2.d. Met with Regulatory Attorneys and noted if the Commission were to adopt a new decision, Regulatory Lawyers would socialize this decision to necessary business groups. It is then the responsibility of the respective business units to implement the decision.	
3. Inspect original and revision dates of policies to assess if actual updates/edits are made before approvals.	3.a. Met with members of the Privacy Team and noted SoCalGas has not made any significant changes to the *Privacy Notice* since 2014. 3.b. Observed email communication from 07/08/2021 evidencing the review and approval of the *Privacy Notice* by Privacy Program Manager. 3.c. Observed communications evidencing there were no changes made to the *Privacy Notice* for 2021 and that it was approved by Privacy Program Manager to be sent to customers.	

Assessment procedures	Assessment test results	Exceptions
4. Assess how SoCalGas informs customers of any alterations to the Privacy Notice and where prior versions will be made available to customers.	4.a. Reviewed the *Privacy Notice* online and noted it informs customers changes to the *Notice* will be made as necessary and will be communicated on SoCalGas' website, socalgas.com. Customers will also be notified annually in a bill insert to revisit the most updated version of the *Notice* on the SoCalGas website. The website provides customers with a telephone number (800-427- 2200 for Residential Customers, 800-427-2000 for business customers), an email address (webmaster@socalgas.com), and a mailing address where individuals can request a current or prior version of the *Notice*. 4.b. Reviewed the *Privacy Policy* online and noted SoCalGas "reserves the right, at any time, and without notice, to add to, change, modify, or update the *Privacy Policy* by posting a revised policy on their website. When an update is posted the date of modification is edited accordingly." The website also provides customers with a telephone number and mailing address where individuals can ask any questions or comments regarding the website *Privacy Policy* or any other questions about the website, SoCalGas, or its services. 4.c. Emailed webmaster@socalgas.com on 10/08/2021 and asked for prior versions of the *Privacy Notice* in effect during the period between 2017 through 2020. Received an email response from SoCalGas' Privacy Team on 10/13/2021 containing the *Privacy Notice* effective since July of 2014.	
5. Observe whether SoCalGas' *Privacy Notice* identifies the title and contact information (including email address, postal address, and telephone number) of an official at SoCalGas, who can assist the customer with potential privacy questions, concerns, or complaints.	5.a. Reviewed SoCalGas' *Privacy Notice* and noted it includes contact information where customers can provide comments and concerns regarding the *Privacy Notice*. The contact information includes an email address (webmaster@socalgas.com), a mailing address directed to the Customer Privacy Program Manager, a Residential phone number (1-800-427-2200) and Business Customer phone number (1-800-427-2000).	
6. Assess whether a specific person or group within SoCalGas is responsible or accountable for privacy and security policy	6.a. Reviewed the SoCalGas *Customer Privacy Program Standard Operating Procedures* and noted SoCalGas created the SoCalGas Customer Privacy Program to ensure proper policies, practices, training, systems, and security practices are in place to protect the privacy of customer data.	

Assessment procedures	Assessment test results	Exceptions
development, implementation, monitoring, enforcing, and updating.	6.b. Reviewed documentation provided by members of the Privacy Team and noted the Customer Services Vice President is the Customer Privacy Officer. Her team is responsible for setting policies, assuring customer data privacy across the organization, and achieving enterprise goals. 6.c. Obtained and reviewed job descriptions for the Privacy Program Team, responsible for privacy and security surrounding covered information, and noted: — The Customer Operations Director is the Director of Customer Privacy and provides oversight for the implementation of customer privacy policy. — The Customer Services Technology Operations & Data Privacy Manager is responsible for working with IS to ensure sound privacy and security controls are adhered to as part of the Data Governance Plan. — The Customer Privacy Program Manager is the "privacy expert" responsible for the day-to-day activities of the Customer Data Privacy Program. i. This individual ensures employees and contractors understand the Privacy Policies regarding customer data; ii. Administers Privacy Impact Assessments (PIAs); iii. Obtains approval from the Director and Chief Privacy Officer for third party data requests when needed; iv. Oversees the Energy Data Request Program (EDRP); v. Leads the annual report filing to the CPUC; and vi. Facilitates the annual independent audit process of Privacy Rules. — The EDRP Administrator is responsible for the day-to-day activities associated with administering both the business process and system associated with EDRP data requests. — All employees handling customer data and Covered Information are obligated to follow Company policies and procedures and are	

Assessment procedures	Assessment test results	Exceptions
	responsible for implementing and monitoring compliance with the *Privacy Policy*. 6.d. Met with SoCalGas' Customer Operations Team and noted ongoing privacy steering meetings and controls are in place. There is an Enterprise Risk Managing Consumer Privacy Risk Team, which oversees controls protecting Covered Information. In addition, SoCalGas' Chief Privacy Officer presents to the Senior Management Steering Team regarding current privacy landscape, current risks, any risk mitigation and remediation occurring, as well as metrics that are published in SoCalGas' *Annual Privacy Report*.	

CPUC RULE 3 – Purpose specification

Overall assessment result	**Exception noted:** SoCalGas' Privacy Notice provided to customers states that the customer may contact SoCalGas if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.

CPUC Rule 3	Rule description	**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.
a(1)-(3)		

Assessment procedures	Assessment test results	Exceptions
1. 1. Assess whether SoCalGas' 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.a. Reviewed the *Privacy Notice* online and noted it provides: — The kinds of information that will be collected from and about customers — How that information will be collected, used, and protected — In what cases customer information will be disclosed to third parties — To whom customer information will be potentially disclosed in the outlined circumstances (e.g., subpoena, emergency responders, as ordered by CPUC or as required by law) 1.b. Met with the Privacy Team and was informed SoCalGas does not share Covered Information with third parties for Secondary purposes. 1.c. Reviewed SoCalGas' *Rule No. 42 Privacy and Security Protections for Energy Usage Data* and noted the document provides the definition of primary uses of Covered Information: — Provide or bill for gas; — Provide for system, grid, or operational needs;	

Assessment procedures	Assessment test results	Exceptions
	— Provide services as required by state or federal law or as specifically authorized by an order of the Commission; or — Planning, implementing, or evaluating demand response, energy management, or energy efficiency programs under contract with the Utility, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission.	
2. Assess whether SoCalGas tracks the categories of agents, contractors and other third parties to which they disclose Covered Information for a primary purpose.	2.a. Reviewed the *List of In-Scope Business Partners/Vendors* and noted the document lists vendors who have access to Covered Information. 2.b. Reviewed SoCalGas' *2020 Annual Privacy Report* submitted to the CPUC and noted SoCalGas disclosed Covered Information to 516 third parties during the 2020 calendar year, which included suppliers, contractors, vendors under contract with SoCalGas, local governments, academic researchers, state and federal agencies who properly requested the data, and customer authorized third parties. 2.c. Reviewed SoCalGas' *Process for Tracking Customer Data Requests* and noted the process for tracking customer data requests for Covered Information when requested by local city governments and agencies. 2.d. Received a written response from a member of the Supply Management Team and was informed the IT VMO leads the guidance regarding performance of systematic assessments and tracking of IT vendors, including those with Covered Information access.	
3. Assess whether a procedure exists to assess whether new customers receive notice of SoCalGas' reasons for collecting, using, storing, or disclosing Covered Information.	3.a. See CPUC Rule 2b(1) Test Results.	
4. Assess whether SoCalGas effectively monitors compliance with its collection, use, storage, and disclosure practices.	4.a. Reviewed SoCalGas' *Customer Privacy Program Standard Operating Procedures* and noted monitoring and enforcement of privacy policies and procedures are components of the Customer Privacy Program.	

Assessment procedures	Assessment test results	Exceptions
	4.b. Met with the Privacy Team and members from the Legal Team and was informed if any changes to CPUC regulations occur, the Legal Team communicates these new regulations to the business unit affected. The business unit is responsible for implementing changes. The Privacy Team tracks yearly compliance with CPUC guidelines. 4.c. Reviewed documentation associated with Internal Audits conducted in 2021 and noted that there were no audits conducted related specifically to Covered Information during 2021. An audit which included systems containing CEUD was conducted during the covered period and no issues were identified. 4.d. Reviewed the *Customer Privacy Compliance Plan* and noted SoCalGas tracks compliance with each section of Rule 42. As of 11/4/2021 this plan included compliant status for all sections except for the "Audit of data privacy and security practices" which was in process at the time, and finalized by KPMG as of the date of this report.	

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' *Privacy Notice* addresses the retention of Covered Information.	1.a. Reviewed the *Privacy Notice* and noted SoCalGas keeps energy usage information "only for as long as necessary to serve customers". The *Notice* also indicates, "retention periods vary based on the specific circumstances and business needs but will most typically be for eight to ten years."	

CPUC Rule 3	Rule description	Customer limitation:
c(1)		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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' *Privacy Notice* and processes address customers' ability to view, inquire, or dispute their Covered Information or other PII.	1.a. Reviewed the *Privacy Notice* and noted it identifies how customers may contact SoCalGas with questions and to find out how they can limit, view, or dispute their disclosed information. Customers can contact SoCalGas by calling 1-800-427-2200 (Residential Customers) or 1-800-427-2000 (Business Customers), emailing webmaster@socalgas.com, mailing the provided address to the Customer Privacy Program Manager, or by signing into the customer's online account at socalgas.com/my-account/ to edit their profile. 1.b. Reviewed SoCalGas' *October 2021 Bill Insert* to customers, which included the SoCalGas *Privacy Notice*. The *Notice* states SoCalGas provides customers with the option to "find out how you can limit, view, or dispute your disclosed information" by contacting SoCalGas at: — Telephone: 1-800-427-2200 (residential) or 1-800-427-2000 (business) — Email: webmaster@socalgas.com — U.S. Mail: SoCalGas, Attn: Customer Privacy Program Manager, P.O. Box 1626, Monterey Park, CA 91754 1.c. Reviewed an example *Account Registration Confirmation* email for residential customers and an *Account Registration Confirmation* email for business customers. These emails contain a link to SoCalGas' privacy center on the homepage of the SoCalGas website. The privacy center contains privacy-related links, including a link to the *Privacy Notice*. This online version of the *Notice* contains a telephone number, email address and postal address customers can use to view, inquire about, or dispute their Covered Information. 1.d. Met with Customer Contact Center Operations Support Manager and Customer Services Technology Advisor for the Customer Contact Centers and was informed when a customer calls with a complaint, the Customer Service Representatives (CSRs) registers it into the Customer Information System (CIS) as either a complaint, compliment, or	

Assessment procedures	Assessment test results	Exceptions
	comment, with the designation of urgent, high, or low. The CSR also indicates what department the complaint belongs to. CIS prepopulates the responsible department, date, and other information, and then routes the complaint to the correct department. Complaints related to customer security or privacy are routed to Residential Marketing, Information Security/ Corporate Security, or the Privacy Office depending on the specific content of the complaint. 1.e. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-427-2200) for inquiries regarding their bills and account management. The customer bill also states if the customer is not satisfied with SoCalGas' response, the customer can contact the CPUC at 1-800-649-7570 or by visiting www.cpuc.ca.gov/complaints/. 1.f. Reviewed the *Customer Complaint Elevation Guidelines* and the *Referral Chart for Elevated Written Complaints* and noted there is a process in place to escalate written, phone, and other customer complaints. 1.g. Reviewed the standard template email SoCalGas sends in response to customers emailing the Privacy Team asking to limit the sharing of their personal information. The standard response refers the customer to the *Privacy Policy* and *Privacy Notice*.	

CPUC Rule 3	Rule description	Customer limitation:
c(2)		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' *Privacy Notice* addresses the explicit/implicit consent required to collect, use, and disclose Covered Information and other personal information.	1.a. Reviewed the *Privacy Notice* and noted it addresses implicit customer consent for primary purposes and explicit consent required for third party information sharing: — Sharing with third parties: SoCalGas may share Energy Usage information with technology providers, consulting organizations, engineering firms, and energy-efficiency providers to better serve customers. — Other Third Parties: SoCalGas may ask customers for permission to share Energy Usage information with other companies required to follow SoCalGas' privacy policies. — Sharing at your choice: Customers can designate third parties to receive their information. — Sharing for other purposes: SoCalGas may release Energy Usage information as required by warrant or subpoena, to emergency responders in the case of imminent threat to life or property, as required by the CPUC, or as required by law. The *Privacy Notice* also addresses customers rights to limit the information provided to SoCalGas. See CPUC Rule 3c(2) Test Results. 1.b. Noted customers can fill out three different forms granting or revoking third parties' access to their Covered Information, depending on type of information and authorization: — CISR Form 8204: Authorization or Revocation to Receive Customer Interval Usage Information — CISR Form 8206: Authorization to Receive Customer Information or Act on a Customer's Behalf	

Assessment procedures	Assessment test results	Exceptions
	— CEC Utility Data Release Authorization Form: Authorization to Release Customer Information to the CEC on a Customer's Behalf for Proposition 39 1.c. The *California Consumer Privacy Act Notice at Collection Standard* requires SoCalGas to inform consumers the type and purpose of personal information collected. The standard then discusses SoCalGas' regulations for notifying customers prior to the collection of personal information. SoCalGas will provide notice to consumers at the point of collection regarding what personal information will be collected and how it will be used on different platforms. 1.d. Met with Customer Services Technical Advisor and was informed if a third-party requests information for a customer, a CISR authorization form must be issued. CISR forms are validated before any information is shared.	
2. Assess whether SoCalGas communicates to individuals the consequences of denying consent.	2.a. Reviewed the *Privacy Notice* and noted customers may dispute, ask questions, or place complaints by contacting SoCalGas through mail, email, or by phone. However, no consequences are stated if the customer chooses to limit their Covered Information. 2.b. Reviewed SoCalGas' Website *Privacy Policy* and noted it states: "[the customer] may choose not to provide any Personal Information and [they] will still be able to access most portions of the web site." 2.c. Reviewed the *Advanced Meter Opt-Out Program* publicly available at SoCalGas.com and noted for customers who do not wish to have advanced meters installed on their homes, they can opt-out by contacting their gas utility provider directly. This web page also includes a FAQ section with details and additional costs associated with opting out.	The SoCalGas Privacy Notice provided to customers states that the customer may contact SoCalGas if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.
3. Inspect SoCalGas' systems where Covered Information is collected to assess whether	3.a. Reviewed SoCalGas' customer account online registration process and noted that to create an account, the customer must check a box acknowledging review and agreement to SoCalGas' My Account Terms	

Assessment procedures	Assessment test results	Exceptions
customers' implicit or explicit consent preferences are captured (before data transfer).	and Conditions, which includes a checkbox to acknowledge and confirm agreement. 3.b. Reviewed SoCalGas' *Website Terms and Conditions* (publicly available at https://www.socalgas.com/terms-and-conditions) and noted: — "Users must discontinue use of this Web site immediately if they do not agree or accept all of these Terms and Conditions." — "Our privacy policy pertaining to any information obtained by Company from this Web site can be found in the Privacy section of the Web site. Additional privacy rules may apply as stated in portions of this Web site restricted for specific User services." 3.c. Reviewed *My Account Terms and Conditions*, which state: "You are subject to these My Account Terms and Conditions as long as you take part in My Account, including all its online services. By selecting the 'I Agree' button when registering for My Account, you are confirming that you accept these My Account Terms and Conditions (or any future modifications thereof) – as a pre-condition to your being granted access to My Account." 3.d. Reviewed the website *Privacy Policy* and noted it states: "By using our website or obtaining any product or service through our website, 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 website." 3.e. SoCalGas' *California Consumer Privacy Act (CCPA) Policy Standard* states: "We are required to notify California residents, at or before the point of collection of their Personal Information, the categories of Personal Information collected and the purposes for which such information is used."	

CPUC RULE 4 Individual Participation (Access and Control)

Overall assessment result	No exceptions noted

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' *Privacy Notice* addresses the provision of access to individuals to their Covered Information.	1.a. Reviewed SoCalGas' *Privacy Notice* and noted that customers can view their energy usage data online accessing *My Account* at www.socalgas.com/my-account/. 1.b. Reviewed *My Account* portal in the link above and noted it provides detailed instructions for customers to register and create an account to retrieve their energy usage data. 1.c. Reviewed SoCalGas' *My Account Registration Confirmation* email and noted it contains a link to *My Account* portal. The email also informs customers they can manage their gas account 24/7 via *My Account*.	
2. Assess whether SoCalGas' internal policies describe the process for providing customers with access to their Covered Information.	2.a. Reviewed the *My Account* registration process and noted for customers to retrieve their energy usage data, they must be authenticated by enrolling and logging into the secure online customer portal. Once customers are authenticated and enrolled, they can view and retrieve their usage data. 2.b. Reviewed the internal *Customer Contact Operating Procedures for Safeguarding Customer Account Information* document detailing how CSSs must authenticate a customer of record or an authorized third-party prior to discussing Covered Information. 2.c. Met with a CSS at the Customer Contact Center and was informed customers can call to request Covered Information. Before any information is shared, the CSS must authenticate the caller by obtaining	

Assessment procedures	Assessment test results	Exceptions
	the name on the account, as well as the bill account number or complete address.	
3. Assess whether customers can access their Covered Information in a detailed, yet easy-to-read format.	3.a. Obtained and inspected a screenshot of a customer's online *My Account* profile and noted customers can access their energy usage information on the portal. Customers can export an *Energy Usage Report* containing up to 24 months of their energy usage data by clicking on the "Export to Excel" link. Customers also have 24-hour access to their energy usage data. 3.b. Reviewed an *Energy Usage Report* excel sample and noted it contains information such as bill date, billed days, gas usage, average therms/day, total gas charges, average $/day, and average daily temperature. This information is presented in a detailed and easy-to-read format. 3.c. Reviewed two sample *Home Energy Reports* and noted they include information comparing the customer's usage details to those of similar homes and to similar homes considered "efficient."	

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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has a process in place for providing customers with access to grant and revoke authorization for secondary uses.	1.a. Reviewed the *Third-Party Requests for Customer Information Standard* and noted SoCalGas requires customer consent to disclose Covered Information to a third party. The standard also provides information on *CISR* forms, which are required to be completed with customer written consent prior to release of Covered Information. 1.b. Reviewed the *Advanced Meter Business Operations Support Authorized Interval Data Request Business Process Design* and noted the process for a Third Party to request interval data on customer accounts with an advanced meter. 1.c. Reviewed the *Customer Correspondence Procedures: Processing Third-Party Requests* and noted the internal procedures followed when a customer or third-party requests to have information sent to a third party. 1.d. Inspected sample *CISR* forms and noted customers must provide consent for disclosure of certain account information for a specified time period to designated third parties. In addition, the customer can revoke authorization at any time by completing the *CISR* form and checking the "revocation" box. 1.e. Met with Customer Services Technical Advisor and was informed if a third-party or an organization requests information for a customer, a *CISR* authorization form must be issued. *CISR* forms are validated by the Correspondence Department before any information is shared.	
2. Assess whether SoCalGas has a process in place for customers to access their Covered Information	2.a. Reviewed the *Privacy Notice* and noted customers have access to their Covered Information through monthly bills and their *My Account* online	

Assessment procedures	Assessment test results	Exceptions
and dispute its accuracy and completeness.	portal. Customers can also contact SoCalGas through phone, web, or mail with questions, concerns, or complaints. 2.b. Obtained and inspected a screenshot of a customer's online account and confirmed customers can access their CEUD through their *My Account* portal. 2.c. Met with Customer Contact Center Operations Support Manager and Customer Contact Center Supervisor and was informed CSSs are trained to help resolve common customer disputes, inquiries, or questions including accuracy and completeness of their information. If the representative is unable to resolve the issue, it is escalated to a supervisor. 2.d. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-427-2200) for inquiries regarding their bills and account management. The customer bill also states if the customer is not satisfied with SoCalGas' response, then the customer can contact the CPUC at 1-800-649-7570 or visit www.cpuc.ca.gov/complaints/.	
3. Assess whether SoCalGas 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. Met with Customer Contact Center Supervisor and Customer Contact Center Operations Support Manager and was informed once the representative verifies a customer calling in as the customer of record, they can assist with making corrections or updates to the customer's account. 3.b. Met with Customer Contact Center Operations Support Manager, Customer Contact Center Supervisor, and Customer Service Technology Advisor and learned a customer can call the Customer Contact Center with a complaint or send an email to the email address posted to the SoCalGas website. When a complaint is related to customer privacy, the complaint is registered into the CIS and then routed to the Residential Marketing team for investigation and resolution. 3.c. Reviewed SoCalGas' *Privacy Notice* and noted customers may contact SoCalGas through phone, email, or mail to limit, view, or dispute disclosed information. 3.d. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-427-2200) for inquiries regarding their bills and	

Assessment procedures	Assessment test results	Exceptions
	account management. The customer bill also states if the customer is not satisfied with SoCalGas' response, then the customer can contact the CPUC at 1-800-649-7570 or visit www.cpuc.ca.gov/complaints/.	

CPUC Rule 4	Rule description	Disclosure pursuant to legal process:
c(1)-(6)		(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 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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has procedures in place to help ensure proper handling and documentation of any Covered Information data disclosures for legal reasons.	1.a. Reviewed SoCalGas' *Privacy Notice* and noted customers are informed SoCalGas may release energy usage information for the following reasons: — pursuant to a legal process (such as a warrant or subpoena), — to emergency responders in the case of imminent threat to life or property, — as ordered by the CPUC, or — as otherwise required by law. 1.b. Reviewed the *Customer Information Processing Standard* and noted SoCalGas will not disclose or share consumer information without customer consent except for the case of specific exceptions or a primary purpose. 1.c. Reviewed SoCalGas' *Rule 42- Legal Process Request Policy and Processes* and noted when a subpoena or legal request includes	

Assessment procedures	Assessment test results	Exceptions
	Covered Information, the SoCalGas Subpoena Department is required to notify customers in writing and allow them seven days to appear and contest the claim. 1.d. SoCalGas' *Rule 42- Legal Process Request Policy and Processes* also states the following steps for responding to a legal request for Covered Information: — Upon receipt of a legal process request, determine if Covered Information is being requested. — If Covered Information is requested, prepare and send a Notice to the customer to inform the customer of the request for Covered Information. If the customer does not respond within seven days, the Covered Information may be disclosed. If the customer does provide a motion or objection, await the outcome prior to disclosing the Covered Information. — If Covered Information is requested by an Investigative Agency, prior to providing the customer notification, prepare a "Notice to Requesting Entity" to inform the entity of Rule 42 and the notice requirement. — Regardless of what is being requested, anytime a legal process response is prepared ensure all Covered Information has been redacted unless the three steps above have been followed. 1.e. Reviewed *Customer Contact Operating Procedures- Safeguarding Customer Account Information* which states: "In general, SoCalGas employees may not disclose customer-specific account information to any third-party, Company affiliate, or government agency (including the Police and Fire Departments) without the customer's prior written consent or subpoena." 1.f. Met with Senior Litigation Paralegal and Senior Litigation Counsel and noted subpoenas are received via mail or fax. All subpoenas are sent to Senior Paralegal within the Law Department. If Covered Information is requested, a *Notice of Disclosure of Energy Usage Data* is sent to the customer and allows seven days for the customers to contest the subpoena. SoCalGas' Law Department manages, tracks, and reports	

Assessment procedures	Assessment test results	Exceptions
	disclosures pursuant to legal process, including the statistics provided in SoCalGas' *Annual Privacy Report*.	
2. Inspect documentation regarding disclosure of Covered Information pursuant to a legal purpose to test whether SoCalGas properly handled the demand.	2.a. Reviewed a redacted customer *Notice of Disclosure of Energy Usage Data* sent to a customer on September 3, 2021. 2.b. Inspected SoCalGas' *Subpoena Log* and noted in 2021, there were 14 subpoena requests. No customers responded to the *Notice of Disclosure of Energy Usage Data*. 2.c. Reviewed a sample letter of the *Notice of Disclosure of Energy Usage Data* sent to specific customer(s) noted in the subpoena prior to SoCalGas disclosing Covered Information. Noted customers are provided a seven (7) day notice to respond to the demand pursuant to SoCalGas' legal process.	
3. Inspect the Annual Report submitted to the Commission to test whether SoCalGas reported the number of demands received for disclosure of customer data pursuant to a legal process and the number of customers whose records were disclosed.	3.a. While the *2021 Annual Privacy Report* is not available as of the date of this report, KPMG had access to and reviewed SoCalGas' *2020 Annual Privacy Report* submitted to the CPUC on April 30, 2021 and noted during calendar year 2020, SoCalGas received and answered nine demands to disclose customer data pursuant to a legal process.	

CPUC Rule 4 d	Rule description	**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).

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has procedures in place to help ensure proper handling and documentation of any Covered Information data disclosures in situations of imminent threat to life or property.	1.a. Reviewed SoCalGas' *Privacy Notice* and noted SoCalGas may disclose Covered Information without customer's prior consent to emergency responders in the case of imminent threat to life or property. 1.b. Reviewed written documentation provided noting the SoCalGas procedures regarding such requests as: — Data requests related to a situation of imminent threat to life or property are directed to Corporate Security. — Corporate Security determines if the request is for customer information and/or Covered Information. — If the request is for customer information and/or Covered Information, Corporate Security directs the requestor to contact Customer Operations Technology or the Law Department. i. If directed to Customer Operations Technology, they will work with the Privacy Team to fulfill this request. ii. If directed to the Law Department, the requestor is informed a subpoena is required.	
2. Inspect documentation regarding disclosure of Covered Information in situations of imminent threat to life of property.	2.a. While there is no formalized documentation regarding the disclosure of Covered Information in situations of imminent threat to life or property, KPMG met with Senior Litigation Paralegal and Senior Litigation Counsel and noted if such request existed, their team would be informed.	
3. Inspect the Annual Report submitted to the Commission to assess whether SoCalGas reported the number of demands received for disclosure of customer data pursuant to	3.a. While the *2021 Annual Privacy Report* is not available as of the date of this report, KPMG had access to and reviewed SoCalGas' *2020 Annual Privacy Report* submitted to the CPUC on April 30, 2021 and confirmed SoCalGas received zero (0) requests to disclose Covered Information pursuant to situations of imminent threat to life or property.	

Assessment procedures	Assessment test results	Exceptions
situations of imminent threat to life or property and the number of customers whose records were disclosed.	3.b. Met with Senior Litigation Paralegal and Senior Litigation Counsel and noted there were no requests due to imminent threat to life or property during 2021.	

CPUC RULE 5 Data Minimization

Overall assessment result	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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas 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 SoCalGas' *Privacy Notice* and noted customer information is kept only for as long as necessary to serve customers and handle matters like billing disputes, inquiries, and system planning. Retention periods vary based on the specific circumstances and business needs, but will most typically be for 8-10 years. 1.b. Reviewed *Rule No. 42 Privacy and Security Protections for Energy Usage Data,* applicable to all SoCalGas employees, and noted SoCalGas has the following data minimization practices in place: — 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* or for a specific secondary purpose authorized by the customer. — 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* or for a specific secondary purpose authorized by the customer. — 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* or for a specific secondary purpose authorized by the customer. 1.c. Reviewed SoCalGas' *Privacy Impact Assessment User Guide* and noted the purpose of the form is to facilitate resolution of privacy risk and compliance challenges in new and updated systems and business	

Assessment procedures	Assessment test results	Exceptions
	processes. The form lists a series of questions to precisely identify the sensitive customer information required to minimize the collection, storage, usage, and disclosure of Covered Information. 1.d. Reviewed the *Consumer Information Processing Standard* available to all SoCalGas employees on the privacy intranet site and noted only the information necessary to complete the transaction or activity required should be collected. Departments collecting consumer information should document how each data element collected will be used and stored. 1.e. Met with Mass Market Credit and Collections Project Manager and Mass Market Credit and Collections Manager and was informed department employees are allowed access to customer information strictly needed to perform their job function. In addition, SoCalGas has data minimization procedures in place, including a clean desk policy in the office and while working from home. When working in the office, supervisors walk the floor to ensure the policy is being followed and to avoid unnecessary documentation and information sharing. 1.f. During a virtual walk-through of SoCalGas' Santa Ana Branch Office, KPMG noted SoCalGas has data minimization procedures in place, including a clean desk policies and employees must badge onto the printers before accessing documents sent to print.	
2. Assess whether SoCalGas has Data Minimization procedures in place as they relate to the collection, storage, usage, and disclosure of Covered Information for Secondary Purposes.	2.a. Met with the Privacy Team and was informed SoCalGas does not disclose Covered Information for Secondary Purposes unless formally authorized by the customer with a *CISR* form.	
3. Assess whether SoCalGas has internal privacy policies addressing Data Minimization.	3.a. Reviewed internal policy documents available to all employees and noted SoCalGas provides *Information Classification Guidelines* which outline the classification levels and the protections required for information at each level. In addition, the guidelines state that generally, information	

Assessment procedures	Assessment test results	Exceptions
	should be limited to the fewest number of individuals to reduce the risk of compromise or misuse. 3.b. Reviewed SoCalGas' *Standard Operating Procedures* and noted it addresses CPUC data minimization regulatory requirements. 3.c. Reviewed the *Sempra Code of Business Conduct* and noted employees are obligated to protect any confidential information they learn or encounter in the workplace. In addition, the code requires limiting access and usage to authorized personnel and only for appropriate business purposes.	
4. Assess whether SoCalGas implements Data Minimization across User Access roles to systems and applications where Covered Information is stored, used, or processed.	4.a. During virtual walk-throughs of the SoCalGas Customer Contact Center and Branch Office observed employees practice data minimization principles and only access the information needed to complete the transaction or activity. 4.a. Reviewed the SoCalGas' *Consumer Information Processing Standard* noted only the information needed to complete a transaction or activity should be viewed or collected.	

CPUC Rule 5	Rule description	**Data retention:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' internal policies address a document retention policy covering all relevant aspects.	1.a. Reviewed SoCalGas' internal *Information Management Policy* which applies to all Sempra employees and noted it includes process of preservation, organization, and disposal of all company related information. This policy also includes recordkeeping requirements designated to ensure records are appropriately classified, stored, and disposed of in accordance with business and applicable legal requirements. The policy includes links to the *Legal Hold and Preservation Policy*, *Information Security and Acceptable Use Policy*, *Information Management* site, and *Approved Information Repositories*, among others. 1.b. Reviewed SoCalGas' *Records Retention Schedule* and noted the schedule provides detailed retention periods for document classifications grouped by business functions, subjects, descriptions, and retention timeframes. 1.c. Reviewed SoCalGas' *Wireless Communication Device Policy* and noted mobile devices are subject to the same retention periods than those stated in the *Information Management Policy* noted above. 1.d. Reviewed SoCalGas' *Data Destruction and Sanitization Guidelines* and noted the document describes guidelines for destroying and sanitizing data to protect customer data from misuse. All data should be securely destroyed after its retention period has ended. All media should be sanitized or destroyed when its data is no longer needed and before being discarded.	
2. Assess whether the SoCalGas retention policies are periodically reviewed and updated where necessary.	2.a. Met with Regulatory Compliance Advisor and was informed the record function (updating policies and record codes) is managed at Sempra corporate level. In addition, each SoCalGas business unit is assigned an Information Coordinator. Records retention schedules for each business unit are reviewed by the assigned Information Coordinators at least	

Assessment procedures	Assessment test results	Exceptions
	annually. The Coordinators ensure their departmental record retention schedule remains accurate and updated. 2.b. Reviewed SoCalGas' *Information Management Policy* and the *Records Retention Schedule* and noted both documents were updated during 2021.	
3. Assess 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 Regulatory Compliance Advisor function and noted the following: — Information Coordinators are assigned to each business unit and they: i. ensure their departmental record retention schedule is updated and records are cleaned up ii. manage shared sites, ensure electronic sites are cleaned up, and manage reports received from electronic records services annually iii. are responsible for providing status on records contained within reports received from electronic records services (for all records retained, a reason should be stated) iv. are required to take the *Records and Information Management Training* annually — An annual clean-up occurs from May to July where every department "cleans up" their records ensuring they are compliant with the *Records Retention Schedule*. Compliance certification for every department occurs annually from September to December. The certifications go through multiple level of approvals, concluding with approval from the Records Office. — Records can be disposed on-site through a third party or electronically. Records disposed are logged, however due to COVID-19, there was an exception for on-site disposal at closed locations during the covered period. These records will be disposed once offices reopen.	
4. Inspect evidence that SoCalGas records are retained and disposed of in compliance with record retention policies.	4.a. Reviewed a sample *Disposal Log* receiving management approval from 7/1/2021. The approved *Disposal Log* states the record title, record series code, record owner, etc.	

Assessment procedures	Assessment test results	Exceptions
5. Inspect evidence that SoCalGas destroys documents that are no longer necessary or when the appropriate retention policy ends.	5.a. Reviewed a sample *On-site Records Disposal Log* and noted management approval was granted on July 13, 2021to properly dispose of records. 5.b. Observed locked shred bins at facilities containing Covered Information during a virtual walk-through of the SoCalGas Customer Contact Center, Branch Office, Credit Operations, and Billing Operations Center). Noted a contracted third party performs on-site shredding of bin contents. If additional shredding is needed, the facility employees will request an additional pick-up from the third party.	

CPUC Rule 5	Rule description	Data disclosure:
c		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.

Assessment procedures	Assessment test results	Exceptions
1. Understand SoCalGas' privacy policies to assess 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.a. Reviewed internal SoCalGas documentation and conducted interviews with SoCalGas personnel and noted information can be shared with third parties via: — *CISR* Form: Customers must sign and approve a CISR form before SoCalGas can disclose Covered Information with a third party — EDRP: SoCalGas can share aggregated and anonymized data with approved third parties — Contractual signed agreements between SoCalGas and approved vendors — As required by the CPUC — As required by legal processes 1.b. Reviewed the *Privacy Notice* and noted SoCalGas describes practices related to sharing personal information with third parties and the reasons for information sharing. Specifically, SoCalGas informs customers: — Primary Purposes: SoCalGas may share Covered Information with vendors under contract, such as consulting organizations, engineering firms, or technology providers — Customer's Choice: Customers can designate Third Parties to receive their Covered Information by providing written consent — Other Purposes: SoCalGas may release Covered Information pursuant to a legal process, to emergency responders in the case of imminent threat to life or property, or as ordered by the CPUC 1.c. Reviewed a list of in-scope vendors identified as third parties with access to Covered Information during 2021 and confirmed there is a process to track third parties with access to Covered Information. Third	

Assessment procedures	Assessment test results	Exceptions
	parties are subject to contractual agreements, as well as to *Sempra's Supplier Code of Conduct*. 1.d. Reviewed CPUC-approved *CISR* forms and noted customers must provide written authorization to SoCalGas to allow a third party to receive customer information or act on the customer's behalf. In addition, the form states what rights are delegated to third parties, what information the third party is entitled to receive and whether the authorization is provided on a one-time basis or on a longer-term basis (limited in duration to three years). 1.e. Reviewed documentation regarding the *Energy Data Request Program* and noted it is a new program providing specific third parties, such as local governments, state/federal agencies, community service development organizations and researchers of accredited academic institutions, access to energy usage and usage-related data without obtaining a non-disclosure agreement (NDA). The data is provided at an aggregate level and using standards set forth by the CPUC. 1.f. Met with Customer Services Technical Advisor and was informed SoCalGas only shares Covered Information to third parties once customer written consent is obtained through the *CISR* process. The customer must designate in the CPUC-approved *CISR* form the type of information shared and the specified time period for sharing the information. Only upon receiving the customer signed *CISR* form will SoCalGas disclose the requested information to the third party and for the designated purpose. 1.g. Reviewed CPUC-approved *CISR* form*s* and noted the information is consistent based on discussions with the Privacy Team and the Customer Contact Center Technical Advisor. 1.h. Reviewed SoCalGas' *2020 Annual Privacy Report* dated April 30, 2021 and noted SoCalGas classified authorized third parties accessing Covered Information as contractors and vendors under authorized SoCalGas contracts. 1.i. Reviewed *Supplier Code of Business Conduct* and noted Sempra instructs third parties to keep nonpublic information confidential. All nonpublic information must be appropriately secured and protected.	

CPUC RULE 6 Use And Disclosure Limitation

Overall assessment result	**Exception Noted:** Sampled SoCalGas contracts executed since the completion of the prior Covered Information assessment and current standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, while one of the sampled vendor contracts executed prior to the effective date of the Privacy Decision and amended in 2014 contains confidentiality language, KPMG observed privacy and security provisions that do not align to formal regulatory requirements.

CPUC Rule 6	Rule description	
c(1)-(3)		**Disclosures to third parties –** **(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 SoCalGas disclosing the Covered Information shall, by contract, require the third party 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 SoCalGas 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.

Assessment procedures	Assessment test results	Exceptions
1. Understand SoCalGas' privacy policies to assess 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.a. See CPUC Rule 5c for test results. 1.b. Reviewed SoCalGas' *2020 Annual Privacy Report* dated April 30, 2021 and noted SoCalGas classified third parties with access to Covered Information into three categories: — Customer authorized third parties — Vendors under contract — Local governments, academic researchers, and state and federal agencies who have properly requested the data	
2. Assess whether SoCalGas informs customers that personal information is disclosed to third parties only for the purposes (a) identified in the Privacy Notice, and (b) for which the individual has provided implicit or explicit	2.a. Reviewed the *Privacy Notice* and noted SoCalGas only discloses customer information to: — Contracted third parties — Parties as ordered by the CPUC — Third parties with customer consent through CISR form	

Assessment procedures	Assessment test results	Exceptions
consent, or as specifically allowed or required by law or regulation before data is disclosed to third parties.	— Legal processes via subpoena or warrant — Emergency responders in cases of imminent threat to life or property 2.b. Reviewed SoCalGas' *CISR Form 8206* and *CISR Form 8204* and noted by completing the forms, customers authorize a specified third party to request and receive the customer data stated on the form. Customers must specify whether this is a one-time authorization, one-year authorization, or determine an expiration date (limited in duration to three years). To complete the forms, customers must provide their signature stating the customer understands they may cancel the authorization at any time by submitting a written request. — *CISR Form 8206: Authorization to Receive Customer Information or Act Upon A Customer's Behalf* collects customer's authorization for a third party to receive customer information or act on a customer's behalf. — *CISR Form 8204: Authorization or Revocation of Authorization to Receive Customer Interval Usage Information* collects customer's authorization or revocation of authorization to receive customer interval usage information. Customers explicitly authorize a third party to request and receive data such as billing history, account information, and usage data. 2.c. Met with members of the Privacy Team and was informed SoCalGas follows *Tariff Rule 42* regarding disclosure of Covered Information. *Tariff Rule 42* states separate authorization must be obtained by customers for all disclosures of Covered Information (except for legal processes, imminent threat to life or property, or as authorized by the Commission). 2.d. Reviewed SoCalGas' *Safeguarding Customer Account Information Procedures*, a document used by CSSs and noted that upon receipt of third-party data requests for customer information, CSSs mail *CISR* forms to customers to acquire authorization. CSSs notify the customers and the third parties that upon receipt and verification of consent, information is released within 10 business days. 2.e. See CPUC Rule 2c(2) for test results.	

Assessment procedures	Assessment test results	Exceptions
3. Assess whether SoCalGas communicates specific instructions for handling personal information and the consequences of improper disclosure to the third-party prior to disclosing the information.	3.a. Reviewed Sempra's *Supplier Code of Business Conduct* and noted the document states policies regarding information protection and confidentiality: — Information may only be used for Sempra Energy business and must be in accordance with all applicable laws, regulations, and contractual obligations. — Nonpublic information could include, but is not limited to, customer, employee, or other business information and should be limited to only information required to perform the contracted work. — Nonpublic information must be kept confidential and only be disclosed to those subject to Sempra's confidentiality provisions if it is necessary for the performance of the Supplier's work. — Nonpublic information must be appropriately secured and protected. — Suppliers will not make any announcements or release any information on behalf of Sempra Energy without prior and appropriately authorized written consent of Sempra Energy. 3.b. Inspected confidentiality and non-disclosure clauses in a sample *Master Service Agreement (MSA)* between SoCalGas and a supplier with access to Covered Information and noted it includes a definition of Covered Information, governance regarding the handling of customer information, and consequences of improper disclosure. 3.c. Inspected confidentiality and non-disclosure clauses in a sample *NDA* between SoCalGas and a supplier with access to Covered Information and noted it includes a definition of confidential information, governance regarding the handling of customer information, and consequences for noncompliance. 3.d. Reviewed an example *Confirmation Letter* sent to a third party once a data request is fulfilled and noted data confidentiality provisions are included. 3.e. Reviewed documentation related to SoCalGas' *Energy Data Request Program* and noted data should be used only for the purpose specified in the request.	

Assessment procedures	Assessment test results	Exceptions
	3.f. Reviewed the *Sempra Procurement Policy* and noted it outlines policies, procedures, and guidance for procurement purposes, and noted contractors are not allowed to commence work until a valid contract is in place. 3.g. Obtained and inspected a sample MSA and NDA executed between SoCalGas and a vendor with access to Covered Information and noted they include confidentiality and data privacy provisions mentioning potential breach of contract damages should the third party not adhere to contract terms. Additionally, the contracts restrict use of confidential information solely for the purposes stated in the contract. 3.h. Met with members of the Privacy Team and was informed vendors and contractors are contractually obligated to abide by corporate privacy and security policies.	
4. Understand whether third-party contracting documentation is consistent with the SoCalGas' policies and procedures.	4.a. Met with members of the Privacy Team, Portfolio Manager for Supply Management, and Value Capability Manager for the Cybersecurity Risk and Compliance Team and was informed of the following: — Legal reviews all technology contracts with a dollar value of $1,000,000 or more. Contractors are not allowed to commence work until a valid contract is in place. — Once a contract is signed, the contracted business unit is responsible for managing and enforcing the contract. — Agreement templates include a confidentiality clause. In addition, technology contacts also include SoCalGas' *Information Security Requirement* legal terms and agreements. — Three different risk assessments may occur before a contract is executed: i. IT VMO Risk Assessment: conducted on all vendors, regardless of type of data shared. ii. IS Risk Assessment: performed based on type of vendor and data shared. In this case SoCalGas takes steps to further understand the criticality of data and relationship with vendor.	

Assessment procedures	Assessment test results	Exceptions
	iii. Cybersecurity Engineering and Consulting (CEC) Risk Assessment: a deeper risk assessment only assessing certain vendors with access to SoCalGas systems containing sensitive information, in which the *Information Security Third Party Assessment and Attestation* form is issued. 4.b. Was informed by the Privacy Team that before onboarding a vendor, basic information is gathered through the *Customer Privacy Third-Party Review Questionnaire* and entered in a database. IT VMO then conducts the IT VMO Risk Assessment in which they ask multiple vetting questions to decide whether further risk assessments, including comprehensive IS/cybersecurity assessments (i.e., IS Risk Assessment or CEC Risk Assessment) and risk ratings, are needed. 4.c. Reviewed the *IS Third Party Assessment and Attestation* form, used in the CEC Risk Assessment, and noted contractors are asked a series of security infrastructure, monitoring, compliance, and data security questions before a contract is executed. 4.d. Reviewed the *Customer Privacy Third-Party Review Questionnaire* used by the SoCalGas Customer Privacy Program and IS Team to perform a review third parties that receive SoCalGas data and noted SoCalGas asks numerous questions relating to the entity's use of customer data before providing data to a third party. 4.e. Reviewed the *Sempra Procurement Policy* and noted contractors cannot commence work until a valid contract is in place. 4.f. Reviewed the *Supplier Code of Business Conduct* which states customer information should only be used for Sempra Energy business and all nonpublic information must be kept confidential. 4.g. Reviewed the *Information Security Requirements,* included in technology agreements, and noted contractors verify that their products contain the necessary security to meet all regulations and laws regarding data protection. 4.h. Inspected *Additional Terms and Conditions* clause included in SoCalGas' standard contract template used when contracting with third parties and noted it includes a confidentiality clause governing the handling of Covered Information. Contractors shall not disclose any confidential	

Assessment procedures	Assessment test results	Exceptions
	information to other third parties, including SoCalGas affiliates that produce energy or energy-related products or services, without prior written consent and approval of SoCalGas or as required by law. The contract template also states a potential breach of contract damages if the third party does not adhere to contract terms. In addition, contractors are required to return or destroy all Confidential Information upon completion of the work or at SoCalGas' request.	
5. Inspect sample evidence of acknowledgments/certifications from third parties regarding compliance with SoCalGas' data privacy policies.	5.a. See CPUC Rule 9c (3b) for test results. 5.b. Obtained and inspected a sample of five executed vendor contracts with access to Covered Information. It is noted that privacy and security provisions exist in contracts; however, language inconsistencies that do not align to formal regulatory requirements were identified in one of the contracts sampled. 5.c. Reviewed two sample *Information Security Requests for Information Security Assessment and Attestation* forms in which SoCalGas asked vendors a series of security questions. Vendors provided responses and signed to attest they provided truthful responses.	Sampled SoCalGas contracts executed since the completion of the prior Covered Information assessment and current standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, while one of the sampled vendor contracts executed prior to the effective date of the Privacy Decision and amended in 2014 contains confidentiality language, KPMG observed privacy and security provisions that do not align to formal regulatory requirements.
6. Assess whether SoCalGas has a process in place to review	6.a. Was informed by the Privacy Team that the CEC team completes the CEC Risk Assessment on a third party if they host or store company	

Assessment procedures	Assessment test results	Exceptions
contract compliance for third parties accessing or receiving Covered Information.	data. Depending on the final risk score, the company will be reviewed every one, three, or five years. Reviews of third parties are triggered if: — a company will host or store data outside of the SoCalGas network — SoCalGas receives a breach notification of a company that hosts or stores SoCalGas data — a vendor with access to Covered Information has a breach 6.b. Inspected contract template *Additional Terms and Conditions* included in contracts between SoCalGas and vendors with access to Covered Information and noted it includes a "Right to Audit" clause in which SoCalGas has the right to conduct compliance reviews, audits, or other verifications on the contracted company. 6.c. Reviewed the *IS Third Party Assessment and Attestation* form and noted it asks a series of security infrastructure, monitoring, compliance, and data security questions the contractor is required to fill out before a contract is executed. 6.d. Reviewed SoCalGas' *Customer Privacy Third Party Review Questionnaire* used by the SoCalGas Customer Privacy Program and Information Security to perform a review on third parties that receive SoCalGas data and noted the document outlines questions regarding the purpose and scope of the data request and the third party's internal procedure for handling sensitive information. The document also states that except required by law, for an outside party who is not currently under contract with SoCalGas, an NDA is required for SoCalGas to share customer information.	

CPUC Rule 6	Rule description	Secondary purposes:
d(1)-(3)		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas engages in Secondary Purposes, and assess 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 SOCALGAS 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. Met with Customer Services Technical Advisor and Customer Operations Project Manager and was informed SoCalGas requires customer consent through a *CISR* form prior to disclosure of Covered Information to third parties. The customer must designate in the CPUC-approved *CISR* form the type of information shared and the specified time period for sharing the information. 1.b. Inspected SoCalGas' *Procedure for Processing Third Party Requests* and noted the Customer Contact Center reviews and processes third-party requests for secondary purposes. The *CISR* form is required to verify authorization from the customer of record to release account information to the third party. 1.c. Reviewed SoCalGas' *Customer Privacy Program Standard Operating Procedures* and noted customer consent through a *CISR form* is required to release to Third Parties any data for a secondary purpose. 1.d. Met with the Privacy Team and was informed SoCalGas does not share Covered Information for Secondary Purposes without customer authorization.	
2. Assess whether SoCalGas has secondary use authorization forms customers sign to	2.a. See CPUC Rule 6c(2b) for test results.	

Assessment procedures	Assessment test results	Exceptions
authorize use of Covered Information for secondary uses.		
3. Inspect evidence that customer consent authorizing use of Covered Information for Secondary Purposes is documented.	3.a. Reviewed SoCalGas' *CISR* Form *8206: Authorization to Receive Customer Information or Act Upon A Customer's Behalf* and *CISR Form 8204: Authorization or Revocation of Authorization to Receive Customer Interval Usage Information* and noted by completing the forms, customers can authorize a specified third party to request and receive the customer data stated on the forms. 3.b. Met with Customer Services Technical Advisor and Customer Operations Project Manager and was informed SoCalGas Correspondence Department processes *CISR* forms. The forms are validated for accuracy and completeness prior to disclosing information to a third party. No exceptions were noted in the *CISR* process during the covered period.	

CPUC Rule 6	Rule description	Customer authorization:
e(1)-(3)		(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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether customers receive the Privacy Notice and must provide separate authorization if information is being used for a new Secondary Purpose.	1.a. See CPUC Rule 5c for test results. 1.b. Reviewed SoCalGas' *Customer Privacy Program Standard Operating Procedures* and noted customer consent through a *CISR* form is required to release data to third parties for a secondary purpose. 1.c. Reviewed SoCalGas' *Customer Contact Operating Procedures,* an internal guidance document followed by Customer Service Representatives, and noted representatives are instructed to inform customers that a completed *CISR* form is required for customer information to be sent to a third party. 1.d. Reviewed the *CISR* form templates and noted customers can provide authorization and consent for disclosure of specific account information to designated third parties for intervals such as single-time consent, one year authorization, or for a specified period of time as designated by the customer (for a period of up to three years).	
2. Understand how customers are notified of their right to revoke any previously granted authorization and the process to do so.	2.a. Reviewed *Privacy Notice* and noted customers are informed they can limit or dispute third parties' use of previously authorized access to Covered Information. 2.b. Reviewed *CISR Form 8204* and *CISR Form 8206* and noted to complete the form, customers must provide explicit consent and sign an	

Assessment procedures	Assessment test results	Exceptions
	acknowledgment clause stating, "I understand that I may cancel this authorization at any time by submitting a written request." 2.c. Met with the Customer Services Technical Advisor and Customer Operations Project Manager and was informed customers can limit the length of their authorization on the *CISR* form. Once a form expires, another form needs to be completed to continue data sharing. To revoke access, the customers can fill out another *CISR* form check the "revocation" box. 2.d. Reviewed SoCalGas' *Customer Privacy Program Standard Operating Procedures* and noted customer consent is required to release any data of a secondary nature to third parties. The document also explains the *CISR* form is a CPUC-approved form collecting customer authorization for SoCalGas to release customer information to a third party. Once a customer revokes their authorization request, revocation is effective immediately upon receipt of the form. 2.e. Reviewed a sample *CISR Form 8206* and noted customers can specify what types of covered information is authorized as well as the duration of authorization. The specific types of information are included to be requested and/or received are: — Customer billing records, billing history and all meter usage data used for bill calculation — EPA Benchmarking — Copies of correspondence in connection with the customers' account — Investigations of the customers' utility bills — Special metering data in association with the account — Rate analysis — Rate changes — Verification of balances on customer accounts and discontinuance notices The specific duration of these requests are for: — Single-use authorization	

Assessment procedures	Assessment test results	Exceptions
	— One-year authorization — Custom authorization up to three years	

CPUC Rule 6	Rule description	Parity:
f		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has a process in place to allow customers to cancel authorization for any Secondary Purposes.	1.a. See CPUC Rule 6e(2) for test results.	

CPUC Rule 6	Rule description	**Availability of aggregated usage data:**
g		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 Covered Information because of the size of the group, rate classification, or nature of the information.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' Privacy Notice or internal policies address the use of aggregate information.	1.a. Reviewed SoCalGas' *Consumer Information Processing Standard* and noted customer information can be released to third parties for legitimate business reasons when it has been sufficiently aggregated, anonymized, or pseudonymized to hide the customer's identity. 1.b. Examined *Rule No. 42- Privacy and Security Protections for Energy Usage Data* and noted SoCalGas is permitted to use aggregated usage data once removed of all personally identifiable information. 1.c. Reviewed the *Energy Data Request Program (EDRP)* document and noted SoCalGas has the EDRP to provide specific third parties access with energy usage and usage-related data. Highly aggregated data is available publicly on the EDRP website. If this publicly available data is insufficient for the third party, additional information can be requested through EDRP for legitimate business reasons. Third parties using this program are local governments, state/federal agencies, community service development organizations, and researchers of accredited academic institutions. The EDRP was created to provide the above mentioned third parties with aggregated (not customer-specific) data that follows the aggregation standard set forth by the CPUC, and for which customer consent is not required.	
2. Assess whether SoCalGas has a procedure in place to help ensure aggregate information does not disclose or reveal specific Covered Information.	2.a. Met with members of the Customer Privacy Team and was informed data shared externally is highly aggregated and mandated by the CPUC. When data is requested, SoCalGas first offers the aggregated data publicly available. A formal process occurs for further data requests, which go through the EDRP. 2.b. Reviewed *Energy Data Request Program (EDRP)* documentation and noted eligible third parties are: — Local governments	

Assessment procedures	Assessment test results	Exceptions
	— State/federal agencies — Community service development organizations — Researchers of accredited academic institutions access 2.c. Reviewed SoCalGas' *Energy Data Request Program (EDRP)* webpage available on SoCalGas' website and noted it contains: — Quarterly reports containing total monthly sum and average of customer gas usage by zip code and customer class (residential, commercial, industrial). These reports follow CPUC procedures regarding aggregation rules and are accessible by the public — Instructions for eligible third parties to submit requests for customized reports of aggregated data — Data request log that allows requestors to see the status of their submitted requests — Link for eligible third parties to submit requests for custom data reports — Summary of aggregation standards 2.d. See CPUC Rule 6g(1) for test results.	

CPUC RULE 7 Data Quality and Integrity

Overall assessment result	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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas' privacy policies address the quality of Covered Information and other Customer PII.	1.a. Reviewed *Sempra Employee Code of Conduct* and noted employees are required to protect the security and integrity of information. 1.b. Reviewed the *Information Protection Standard* and noted the Information Owner of each business unit is a manager or director responsible for protecting Information Assets. 1.c. Reviewed the *Consumer Information Processing Standard* and noted employees and contractors are to ensure they collect, store, use, and disclose accurate consumer personal information. 1.d. Reviewed *Supplier Code of Conduct* and noted third parties are required to maintain accurate records and disclosures.	
2. Inspect sample communication to customers to assess whether SoCalGas policies include customer data integrity.	2.a. Reviewed SoCalGas *Privacy Notice* and noted customers can limit, view, or dispute their disclosed information by contacting SoCalGas at: — Email address: webmaster@socalgas.com — Mailing address to the Customer Privacy Program Manager — Residential Telephone: 800-427-2200 2.b. Reviewed screenshots of the setup process of the *My Account* portal and noted before customers can create an account, they must check a box acknowledging they have read the *My Account Terms and Conditions*, which states the customers have read and agreed to comply with the *My Account Terms and Conditions* addressing it is the customers' responsibility to provide accurate and up-to-date information. 2.c. Reviewed SoCalGas Website *Terms and Conditions* and noted a "User Account" section which places the responsibility for preserving the	

Assessment procedures	Assessment test results	Exceptions
	confidentiality of log-on and user account information on the customer. The website *Terms and Conditions* also prompts customers to contact SoCalGas with any questions or comments.	
3. Assess 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. Reviewed *Customer Privacy Program Standard Operating Procedures* and noted SoCalGas informs its employees to limit the amount of personal information collected, accessed, used, and stored to only what is required to perform documented business processes. Customer information is to be securely disposed of once the retention period has ended. 3.b. Reviewed *Sempra Information Management Policy* and noted employees must read and certify they have read the policy and will dispose of information accordingly. 3.c. Reviewed SoCalGas *Consumer Information Processing Standard* and noted employees and contractors are to ensure the consumer personal information they collect, store, use, and disclose is reasonably accurate.	
4. Inspect sample evidence to assess whether procedures are in place to safeguard 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.	4.a. Reviewed SoCalGas *Privacy Notice* and noted retention of energy usage data and personal information is addressed: "SoCalGas will keep your Energy Usage information only for as long as necessary to serve you and handle matters like billing disputes, inquiries and system planning. Retention periods vary based on the specific circumstances and business needs, but will most typically be for eight to ten years." 4.b. Inspected the *My Account* registration process and noted customers must agree to provide accurate and up-to-date information. 4.c. Met with Billing Operations team members and was informed when SoCalGas processes bills, validations are run against the data. If data fails the validation, an exception occurs and is reviewed by a member of the billing team to be resolved. There is a process is in place requiring a certain level of supervisor approval depending on the dollar value adjustment associated with the usage read and billing amount. 4.d. Reviewed SoCalGas' *Safeguarding Customer Account Information Procedures* and noted employees are instructed with guidelines and procedures to reinforce SoCalGas' existing policy on confidentiality of	

Assessment procedures	Assessment test results	Exceptions
	customer specific information, and to not disclose customer specific information to any third party, SoCalGas affiliate, or persons not acting as the customer's agent without the customers' prior written consent or a subpoena. 4.e. Reviewed SoCalGas' *Consumer Personal Information Categories and Deletion Exception Standard* which describes the lists and categories of consumer personal information and SoCalGas processes for any exceptions to regular retention schedules.	

CPUC RULE 8 Data Security

Overall assessment result	No exceptions noted

CPUC Rule	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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has documented policies addressing security provisions for Covered Information: — Risk assessment and treatment — Security policy — Organization of information Security — Asset management — Human resources security — Physical and environmental security — Communications and operations management — Access control — Information systems acquisition, development, and maintenance — Information security incident management	1.a. Risk Assessment and Treatment – Reviewed the *Cybersecurity Engineering & Consulting - Risk Rating Procedure* and noted that there is a detailed security risk assessment methodology with the objective of determining the level of risk presented to the organization. This is accomplished through an interview process between CEC, the project team, and key business stakeholders. This document also explains the procedure and remediation plans based on each Common Vulnerability Scoring System scoring model score. This policy is applicable and accessible to all employees of Sempra Energy and is published on the Sempra IS intranet site. 1.b. Risk Assessment and Treatment – Reviewed the *Risk Management Guide* and noted that Sempra has a comprehensive *Risk Assessment Guide* with complete instructions for completing risk assessments, developing a risk response strategy, and monitoring and reporting risk status. Metrics are formally documented and aligned to ISO 31000 principles and guidelines. It was also noted that the risk assessment process is conducted on an annual basis. This policy is applicable and accessible to all employees of Sempra Energy and is published on the Sempra IS intranet site. 1.c. Security Policy – — Reviewed *the Cybersecurity Awareness Standard, Physical Security Policy,* and the *Corporate Security Standards*, and noted that these policies outline access controls to company facilities, conditions for entry, access control practices, badge access authorization, and security planning and equipment. The policies are published on the	

Assessment procedures	Assessment test results	Exceptions
— Business continuity management — Compliance	Sempra IS intranet site accessible to all Sempra employees, vendors, and contractors. — Reviewed the *Sempra Information Security SharePoint site* and noted that company's *Cybersecurity Policy & Procedures site* is accessible to all Sempra employees, vendors and contractors and also includes various cybersecurity policies, standards, guidelines, and procedures. 1.d. Organization of IS – Sempra Energy's IS is structured as a shared service for SoCalGas, SDG&E, and other nonregulated companies. Leadership starts from the C-Suite and flows down throughout the organization. There are cyber councils comprised of senior leadership that meet monthly to raise awareness and discuss the current threat landscape. The IS function is broken down into four main categories 1) Governance Risk & Compliance (GRC), 2) Monitoring & Response (Operations Side), 3) Architecture & Engineering, 4) Program Management (Project and equipment, Capital Expenditure). The program is aligned to the National Institute of Standards and Technology Cybersecurity Framework. 1.e. Asset Management – Reviewed the *Hardware Asset Management Process* and the *Data Destruction & Media Sanitation Guidelines* and noted that these policies describe in detail the process for tracking the lifecycle of hardware IT assets throughout the assets lifecycle. These policies describe in detail the process by which Sempra employees and all affiliates shall handle data storage locations, retentions periods, data classifications, and the methods of destruction for each type of classified data, including Covered Information. The policies are applicable and accessible to all employees of Sempra Energy and are published on the Sempra IS intranet site. 1.f. Human Resources Security – Reviewed the *Employment Verification and Reference Checks Policy & Employment Eligibility & Hiring of Relatives Policy* and noted that there are requirements for preemployment background checks and reference checks and preemployment drug screening. These policies are applicable and accessible to all employees of Sempra Energy and are published on the IS Security intranet site.	

Assessment procedures	Assessment test results	Exceptions
	1.g. Physical and Environmental Security – Reviewed the *Physical Security Policy & Corporate Security Standard* documents and noted that physical and environmental security requirements are formally documented. 1.h. Communication and Operations Management – — Reviewed the *Encryption Standard* and noted that encryption requirements and remote access encryption requirements are formally documented. — Reviewed the *Email Management Standard* and noted that requirements for managing email communications are formally documented. — Reviewed the *Social Media Guidelines* and noted that expectations around Sempra personnel conduct while engaging in social media activity that relates in any way to Sempra Energy are formally documented. 1.i. Access Control – Reviewed the *Electronic Access Management Standard* and the *Identity & Access Management (IAM) Cybersecurity Standard* and noted that access control requirements are formally documented. 1.j. Information Systems Acquisition, Development, and Maintenance – Reviewed the *IT Portfolio Management Office (IT PMO) SharePoint site* and noted that the information systems acquisition, development, and maintenance process are formally documented. 1.k. IS Incident Management – Reviewed the *Cybersecurity incident Response Standard* and noted that cybersecurity incident management procedures are formally documented. 1.l. Business Continuity Management – Reviewed the *Information Technology Disaster Recovery Policy*, as well as the *Business Continuity Policy* and noted that business continuity management and IT disaster recovery requirements are formally documented. 1.m. Compliance – Reviewed the *Supplier Code of Business Conduct*, the *Information Security Policy,* and the *Information Protection Standard* and noted that the requirements for compliance with applicable privacy legislation and regulations are formally documented.	

Assessment procedures	Assessment test results	Exceptions
2. Assess whether SoCalGas' privacy policies and procedures cover protection of electronic and print media containing Covered Information from unauthorized access, destruction, use modification or disclosure.	2.a. Reviewed the *Privacy Policy* and *Information Security Policy* and noted that these policies address how SoCalGas employees, contractors and third parties should handle Covered Information. 2.b. Reviewed the *Data Destruction and Media Sanitation Policy* and noted that these policies describe in detail the process by which Sempra employees and all affiliates shall handle data storage locations, retentions periods, data classifications, and the method of destruction of Covered Information.	
3. Assess 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. Reviewed the *Information Management Policy* and noted that all directors (and managers reporting to VPs) and above shall certify annually that their department is in compliance with the policy. 3.b. Reviewed the *Code of Business Conduct* and noted employees are required to complete compliance training and to acknowledge that they understand and will comply with the Code. Failure to adhere to the standards of conduct outlined in the Code could result in disciplinary action, up to and including employment termination. 3.c. Reviewed the *Risk Exception SharePoint Site* as well as the *Exception Form Sample* and noted that a formal exception is required to be submitted by risk owners who request exceptions from Sempra policies, procedures, standards, or requirements and must include a business justification and mitigation steps. Risk exceptions will expire after one year of the exception approval and require an annual extension if the requirement cannot be met.	
4. Review evidence of SoCalGas providing customers with the Privacy Notice on the security mechanisms used by SoCalGas to protect their Covered Information.	4.a. See CPUC Rule 2b for test results. 4.b. Reviewed the SoCalGas *Privacy Notice* that is available on *https://www.socalgas.com/privacy-notice* and noted that it addresses the security mechanisms used by SoCalGas to protect Covered Information. 4.c. Reviewed the *Privacy Policy* and noted that "Sempra and its Sempra Companies respect the privacy of every employee and customer and collects and retains private, personal information only as required by law or for the company to operate effectively. We must protect and limit access to personal employee, business partner and customer	

Assessment procedures	Assessment test results	Exceptions
	information, limiting access and usage only to authorized personnel and only for appropriate business purposes."	
5. Review evidence that SoCalGas' policies on Data Security are communicated to internal employees and contractors who have access to Covered Information.	5.a. Reviewed the *Information Security Policy* and the *Privacy Policy* and noted that these policies are published on the Sempra IS intranet site, which is accessible to all Sempra employees and contractors with network access, and it provides guidance on data privacy for Sempra Energy. 5.b. Reviewed the *Confidentiality Policy* and noted it is published on the Legal intranet site accessible to all Sempra employees and noted that " Sempra and the Sempra Companies respect the privacy of every customer. Sempra and the Sempra Companies collect and retains a certain amount of customer-specific information that is required to effectively provide reliable, safe, and cost-effective services for our customers. Sempra and the Sempra Companies have implemented policies and procedures that protect and limit access to customer-specific information and comply with all applicable laws that govern confidential customer information." 5.c. Reviewed the *Cybersecurity Awareness Standard* and noted that the company provides employees and contractors with ongoing cybersecurity education and training. The program includes Cyber Champions, who are volunteers trained to foster strong relationships and communicate cybersecurity best practices throughout the organization.	
6. Assess whether a management procedure is in place to monitor whether SoCalGas manages its security program to help ensure the protection of Covered Information.	6.a. See CPUC Rule 8a (1d) for test results. 6.b. Met with Cybersecurity Risk & Compliance Manager and was informed that a cybersecurity operations team and CEC team have been established. The team provides regular updates on identified risks (e.g., cyberattacks, data loss) and the mitigation efforts. 6.c. Reviewed *the Cybersecurity Engineering & Consulting - Risk Rating Procedure* and noted that the team maintains risk management process for making management decisions on security, privacy, and risks. Formal approvals from Cybersecurity and Privacy teams are required prior to new production releases and upgrades. If a project does not meet the necessary cybersecurity control requirements, then a risk exception is documented and sent for review and approvals.	

Assessment procedures	Assessment test results	Exceptions
	6.d. Reviewed the *Risk Management Handbook* and noted that it provides guidance to Sempra on how to implement the risk management framework. It was also noted that an annual risk assessment is required and along with regular vulnerability assessment scans on all systems storing Covered Information. 6.e. Reviewed the *System Monitoring Standard* and noted that Sempra has established and maintains a compliance monitoring and audit program.	
7. Review SoCalGas' relevant policies to assess if SoCalGas incorporates security into their SDLC.	7.a. Reviewed the *Release and Environment Management Standard* and noted that all software development must comply with secure coding principles and practices throughout the stage gates across the SDLC. The requirements include secure coding, development and testing practices, security architecture design, and vulnerability management. 7.b. Met with Cybersecurity Risk & Compliance Manager as well as others from application/web development teams and was informed that Sempra uses an agile DevSecOps methodology, where security is moved forward within the SDLC to ensure security is incorporated into the process. Product owners and scrum masters will obtain the necessary approvals from the Cybersecurity and Privacy teams throughout the process. 7.c. Reviewed the *Information Security Engineering & Consulting Process* and noted that it applies to all types of IT products including software development and technology infrastructure. There are eight (8) phases, from concept to implementing into production and each phase details the purpose and IS supporting activities. The process also includes roles and responsibilities.	
8. Assess whether SoCalGas uses appropriate facility entry controls to limit and monitor physical access to systems and locations where Covered Information is processed and stored.	8.a. Review of the supporting documents *Physical Security & Corporate Security Policy* and noted that the physical access controls are in place to protect Covered Information. 8.b. Reviewed the *Sempra Information Security intranet site* and noted the following controls are in place to protect Covered Information: — Access is controlled by badge access readers — Visitor sign-in and escort procedure — Visitor/Parking forms to identify and track visitors entering the facility	

Assessment procedures	Assessment test results	Exceptions
	8.c. Reviewed the *Sempra Information Security intranet page* and noted the following controls are in place to protect Covered Information: — Access management — On-site guard services — Security training — Risk and intelligence analysis 8.d. Met with Corporate Security Manager and was informed that physical access controls are in place to protect Covered Information. Performed virtual site walk-throughs of the Sempra Production Data Center, SoCalGas Customer Contact Center, and SoCalGas Billing Center and observed that the following controls are in place: — Security guards are on-site 24/7 — Access is controlled by badge access readers — Visitor sign-in and escort is required — Clean desk/Clear screen policy — Covered Information is stored in locked cabinets — Office printers require secure print functionality to complete a print job — Shredders and locked shred bins are located in the facilities	
9. Assess whether SoCalGas has implemented procedures for protecting Covered Information including controls for physically securing all media.	9.a. Reviewed *Information Protection Standard* and noted that portable storage devices must be secured in a locked room, drawer, cabinet, or safe when not in use or unattended. 9.b. Reviewed the *Information Security Manager & User Standard* and noted that user requirements are outlined for actions that must be taken by any user to protect information and technology assets, including physically securing and encrypting media.	
10. Inspect whether physical records containing Covered Information are stored in locked cabinets or rooms restricting unauthorized access.	10.a. Performed virtual walk-throughs of key facilities such as SoCalGas Customer Contact Centers, Branch Offices, and the Sempra Production Data Center and observed that badge access readers are installed throughout the facilities that may limit access to a particular area containing Covered Information. There are secure bins located	

Assessment procedures	Assessment test results	Exceptions
	throughout the facilities for securely discarding any sensitive information therein.	
11. Inquire of SoCalGas' personnel to gain an understanding of the logical control procedures in place to prevent unauthorized access to Covered Information.	11.a. Met with IAM Manager and was informed that a privileged access management solution has been implemented which also provides password management and privileged session recording. The solution has been expanding to encompass more applications and business units. Further, additional logical controls have been implemented, including: — Access requests must be approved by system and information owners — Access accounts are provisioned based on a principle of least privilege — User access accounts are reviewed on a periodic basis	
12. Inspect evidence that logical controls are in place to prevent unauthorized access to Covered Information including user access provisioning and deprovisioning.	12.a. Reviewed the *Electronic Access Management Standard & Service Account & Intelligent Automation ID Guidelines* and noted that formal procedures are in place to help ensure authorized access and prevent unauthorized access. 12.b. Reviewed one (1) sample user access requests and one (1) sample user access removal for a system storing Covered Information and noted that an email chain is used to process the requests. Reviewed screenshots of the user profiles before and after the access requests and access removals and noted that the users were provisioned and deprovisioned in accordance with documented policies and procedures. 12.c. Inspected system profiles for SoCalGas in-scope systems storing Covered Information and confirmed that logical access controls are implemented on the systems in alignment with Sempra policy requirements.	
13. Review SoCalGas' relevant policies to assess if physical controls are in place protecting Covered Information.	13.a. Reviewed the *Physical Security Policy* and noted that controls around the physical protection of Covered Information are documented, including responsibility for managing access to facilities and performing continuous monitoring of facility perimeter controls. 13.b. Reviewed the *Enterprise Records and Information Management (ERIM) Standard* and noted that the operations group within ERIM is responsible for managing physical records storage, including records with Covered	

Assessment procedures	Assessment test results	Exceptions
	Information. This includes maintaining a chain of custody and taking appropriate security and fire-retardant measures. 13.c. Performed virtual site walk-throughs of the SoCalGas Customer Contact Center, a Branch Office, and the Sempra Production Data Center that store Covered Information and observed that the physical access controls implemented were in alignment with Sempra policy requirements. 13.d. Validated through a virtual site walk-through of the Sempra Bill Print facility that the print operators could not see the Covered Information during the bill print and mail insert processes.	
14. Inquire of SoCalGas' personnel to gain an understanding of the controls protecting physical access to systems storing Covered Information.	14.a. Met with Data Center Facility Manager and was informed that the following physical security controls are in place: — Access to the facility is restricted and the front entry gate is equipped with access readers and motion detectors. The main front entrance door has an access reader and a mantrap. Cameras are placed throughout the facility and monitored by an on-site, manned guard station. — Access to server rooms is restricted by a dedicated fence surrounding area and maintained by an electronic access management system. — Employees not assigned to the facility, contractors, and visitors are required to sign a visitor sheet and are escorted throughout the facility.	
15. Inspect evidence that physical access to sites and systems storing Covered Information is monitored and restricted.	15.a. See CPUC Rule 8a (14) for test results.	
16. Review SoCalGas' relevant policies to assess if environmental controls are in place.	16.a. Reviewed the *Sempra Energy Utilities Critical Facilities Standards* and noted the following environmental controls implemented: — HVAC with chilled water to keep the temperature at an appropriate level — Condensers	

Assessment procedures	Assessment test results	Exceptions
	— Fire detection system, alarms, and fire suppression using a Halon and Sapphire system and sprinklers — Backup power supply and generators — Emergency power shutoff, and leak detection	
17. Inquire of SoCalGas' 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. Reviewed the *IT Disaster Recovery Policy* and noted that each tier includes recovery time objectives (RTOs), recovery point objectives (RPOs) impact descriptions, and recovery services. The policy also outlines roles and responsibilities. 17.b. Met with Data Center Facilities Manager and was informed that the appropriate environmental controls in place at the Production Data Center. 17.c. Performed a walk-through of the Sempra Production Data Center and observed the environmental controls implemented are in alignment with Sempra policy requirements.	
18. Assess whether SoCalGas has the ability to transfer data to third parties using secure channels.	18.a. Met with Customer Services Technology Manager and was informed that a third-party risk review process is required to be completed as part of new vendor approvals, including a PIA and an IS risk assessment if they have access to any customer or employee information. 18.b. Met with Cybersecurity Risk & Compliance Manager and was informed that that there are multiple secure file transfers methods used by Sempra, and between Sempra and its third parties. 18.c. Inspected system profiles for systems storing Covered Information and noted that the various systems are configured to provide/support protocols for secured authentication methods.	
19. Assess whether SoCalGas 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	19.a. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that Sempra uses an Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). The IPS/IDS is deployed at multiple points on the network via next-generation firewalls. Logs are sent to Security Information and Event Management (SIEM) tool and all alerts are monitored and reviewed by a 24/7 SOC.	

Assessment procedures	Assessment test results	Exceptions
boundaries and block such transfers while alerting information security personnel.	19.b. Met with Cybersecurity Operations Manager and was informed that there are controls in place to monitor attempts to exfiltrate data across the network boundaries: — A data loss prevention (DLP) tool is implemented to detect data leakage and exfiltration attempts of Covered Information across the network boundaries. — Once flagged, a DLP Analyst will review the incident and determine if it is a true positive. If a true positive is found, the incident is escalated to the appropriate departments. Any follow-up actions that may be needed are determined by Cybersecurity team. 19.c. Observed that the DLP tool is configured to flag instances of unauthorized data exfiltration across the network. 19.d. Reviewed the *Mobile Device Management Standard* as well as the *End User Computing Device Policy* and noted that mobile device management tool is implemented to manage mobile data leakage.	
20. Assess whether SoCalGas 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 while alerting information security personnel.	20.a. See CPUC Rule 8a (19) for test results.	
21. Assess whether SoCalGas has controls in place so that users cannot disable and modify security products or services.	21.a. Reviewed the *Information Security Manager & User Standard* and noted that there are policies in place prohibiting users from circumventing or disabling any technology asset security controls or configurations and from preventing automated updates or scans. 21.b. Met with Cybersecurity Operations Manager and was informed that the DLP agent and antivirus agents are installed on every workstation and a daily health check is reported on the agent's health. It was noted that	

Assessment procedures	Assessment test results	Exceptions
	users do not have administrative access to disable or modify agents on workstations. 21.c. Inspected system profiles for systems storing Covered Information and noted that the various systems are configured with audit logging capabilities to detect system activity. In addition, audit logs are sent to the Sempra SIEM tool for centralized monitoring.	
22. Assess whether SoCalGas officials understand the current threat landscape and potential threats to the organization by leveraging multiple threat feeds.	22.a. Met with Threat Vulnerability Management Manager and the Cybersecurity Risk & Compliance Director and was informed that there is a dedicated cyber threat Intelligence team that provides daily and weekly briefs to stakeholders documenting major events and threat hunting activities. Threat intelligence feeds are digested from a variety of sources including law enforcement, industry sources, and industry sharing forums. Threat sources are aggregated and correlated using enterprise security tools and reports are generated for various needs. In addition, analysts monitor the system continuously and address all items based on priority and triage and escalate the incidents based on information available to them, using detailed playbooks.	
23. Assess whether SoCalGas scans source code for bugs and vulnerabilities before moving it into production.	23.a. Reviewed the *Information Security Engineering & Consulting Process* and noted that as part of the Information Technology Product Lifecycle security testing and assessments are performed to resolve risks and prepare for moving to production. Supporting artifacts, including scan results, source code, technical analysis is documented and reviewed prior to deployment into production. The Cybersecurity team works with vendors to remediate or mitigate all vulnerabilities.	
24. Assess whether SoCalGas' development/test environments are separate from the production environment, with access control in place to enforce the separation.	24.a. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that development, test, and QA environments are separated from the production environment using firewalls and access controls. 24.b. Inspected systems profiles for systems storing Covered Information and noted that they have separate environments for development, testing, production and/or quality assurance purposes. 24.c. Reviewed the draft *Nonproduction Environment Standard* and noted that production data should not be used in nonproduction environments, only testing and dummy data can be used in nonproduction environment. In	

Assessment procedures	Assessment test results	Exceptions
	addition, no customer PII, Internal, Confidential or Restricted data can be used in nonproduction environments.	
25. Assess whether SoCalGas does not use Production Covered Information for testing or development. Test data and accounts are removed before a production system becomes active.	25.a. See CPUC Rule 8a (24) for test results. 25.b. Reviewed the *Release and Environment Management Standard* as well as the *Information Protection Standard* and noted that there are protection standards in place based on information classification that must be adhered to, regardless of the location of that information in the network. Covered Information requires the highest level of protection when stored, accessed, disclosed, transported, or disposed.	
26. Assess whether SoCalGas utilizes a Data Masking tool to limit access to and protect Covered Information and other PII.	26.a. Performed virtual walk-throughs of the SoCalGas Customer Contact Center and Branch Office and was informed that PII is masked, and minimal information is obtained by customer service representatives to perform their tasks. For example, once a social security number has been entered into the system, only the last four characters will remain visible to the agent while the rest will be hashed out.	
27. Assess whether SoCalGas' web applications use encryption when transmitting sensitive data across the network.	27.a. Reviewed the *Encryption Standard* and noted that information classified as confidential or restricted must be encrypted at all times (using the documented minimum encryption strength and protocols), while internal information must be encrypted when transported outside of the company. 27.b. Reviewed the *Information Protection Standard* and noted that all confidential and restricted information must be encrypted at rest and while in transit when moving internally and externally outside SoCalGas's network. 27.c. Inspected systems profiles for systems storing Covered Information and noted that encryption-in-transit protocols are in place to safeguard Covered Information.	
28. Assess whether SoCalGas has implemented an Intrusion Detection system within the environment to detect and	28.a. Reviewed the *Network Security Standard* and noted that network based IPS sensors are deployed inline on the dematerialized zone (DMZ) and secure zone network connection points that can prevent, capture, inspect network traffic for unusual attack mechanisms and detect compromise of	

Assessment procedures	Assessment test results	Exceptions
generate log messages detailing events.	systems through the use of signatures, network behavior analysis and other mechanisms to analyze traffic. 28.b. Met with Cybersecurity, Risk & Compliance Domain Architect and confirmed that Sempra uses an IPS and IDS. The IPS/IDS is deployed at multiple points on the network via the next-generation firewalls at both the network perimeter as well as at several points internally. The generated logs are sent to SIEM tool.	
29. Assess whether SoCalGas has implemented an Intrusion Prevention system within the environment to detect events and reject packets.	29.a. See CPUC Rule 8a (28) for test results.	
30. Assess whether SoCalGas allows only limited access to network resource to vendors and third parties.	30.a. Reviewed the *Electronic Access Management Standard* and noted that contractors and vendors can be issued accounts for a defined period of time. In addition, the standard states that the principle of least privilege must always be used when establishing accounts. 30.b. Met with Supply Management Manager and Cybersecurity & Risk Manager and was informed that all third-party vendors are required to complete security risk assessments before onboarding any new vendors.	
31. Assess whether SoCalGas has a formal process for approving and assessing all network connections and changes to the firewall and router configurations.	31.a. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that Sempra has a formal process in place for approving connections and changes to firewall and router configurations. 31.b. Reviewed the *Sempra Change Management SharePoint page* and noted that all changes and clearances to Sempra IT production environments and systems must have an approved change request. The goal of the Sempra IT Change Management Process is to ensure proper planning, impact assessment, risk assessment, testing, coordination, and approval in order to minimize the risk to production and business processes associated with implemented changes.	

Assessment procedures	Assessment test results	Exceptions
32. Assess whether SoCalGas' firewall performs stateful inspection (dynamic packet filtering) to restrict network access.	32.a. Reviewed the *Firewall Standard* and noted that that Sempra employs firewalls that are capable of stateful protocol analysis and provide intrusion detection or prevention technology. 32.b. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that that Sempra uses next-generation firewalls that apply stateful protocol (dynamic packet filtering) to block unauthorized network traffic.	
33. Assess whether SoCalGas has implemented a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	33.a. Reviewed the *Firewall & Network Security Standard* and *Smart Meter Master Network Diagram* and noted that the use of an DMZ is required to manage communications between Sempra networks and untrusted networks and the Internet to limit inbound traffic.	

CPUC Rule 8	Rule description	**Notification of breach:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas 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 SoCalGas' *Personal Information Breach and Notification Response Plan* and noted procedures to follow if an information breach occurs, including response team roles, documentation of the process, investigation into breaches, remediation, notifications sent, and program updates. Specific procedures are also mentioned if an information breach were to occur within a third-party vendor. In certain cases, an information breach within a third-party vendor could lead to contract termination. 1.b. Met with Chief Counsel for Technology and Business Services and noted he receives a series of monthly reports detailing any unauthorized disclosures (including Covered Information) from the Cybersecurity Group. 1.c. Met with Strategy and Operations Manager for Digital Enablement Services and noted vendors are expected to self-report breaches. 1.d. Met with Portfolio Manager for Supply Management and Value Capability Manager for Cybersecurity Risk and Compliance and was informed if a breach were to occur, the Cybersecurity Team would investigate the incident to find out what occurred, understand the risk, and ask the vendor to provide an explanation. 1.e. Met with Value Capability Manager of Cybersecurity Risk and Compliance and noted if a third-party breach occurred, SoCalGas would immediately disable the vendor's access to SoCalGas online environment. After a breach investigation is completed, SoCalGas' Investigation Team meets with the security teams involved and discusses the investigation and how to improve processes and avoid further occurrences. SoCalGas is constantly updating or creating "playbooks" for incident management as new situations arise.	

Assessment procedures	Assessment test results	Exceptions
2. Assess whether SoCalGas' management has adequately reviewed the incident review process in place.	2.a. Met with Value Capability Manager of Cybersecurity Risk and Compliance and was informed the *Personal Information Breach and Notification Response Plan* is reviewed annually and updated as necessary. 2.b. Met with Value Capability Manager of Cybersecurity Risk and Compliance and was informed after a breach investigation is completed, SoCalGas' Investigation Team completes an investigation review and updates the processes and procedures accordingly. 2.c. Reviewed a list of numerous incident responses in the eGRC system and noted the incident remediations aligned with the *Cybersecurity Incident Response Standard*.	
3. Assess whether SoCalGas can perform forensic analysis in the instance of a Covered Information data incident.	3.a. Met with Cybersecurity Operations Manager and was informed that forensics analysis is conducted in-house and can be performed in the event of an incident involving customer PII or Covered Information. Further, there is a contract in place with a third party in case forensic assistance is needed.	
4. Inspect sample evidence of breach incidents for the last 12 months.	4.a. Met with Value Capability Manager of Cybersecurity Risk and Compliance and observed via shared screen a sample low-level unauthorized disclosure of Covered Information breach incident. 4.b. Reviewed a sample privacy incident involving customer information and noted the investigation process uses a built-in workflow within the eGRC tool. The tool documents information including description, severity, justification, case number, status, legal, supporting documentation, and case logs. The Privacy Team, Information Security, and Legal can collaborate in the tool until in the incident is closed.	

CPUC Rule 8	Rule description	**Annual report of breaches:**
c		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas tracks the reporting requirement and assigns responsibility and accountability to the appropriate departments.	1.a. Reviewed the *2020 SoCalGas CPUC Annual Privacy Report: Schedule/Plan* and noted SoCalGas follows a schedule to file the *Annual Privacy Report* by the due date as required by the Commission. 1.b. Reviewed SoCalGas' *Customer Privacy Compliance Plan* and noted it includes monitoring compliance for each section required by the *CPUC Privacy Decision*, including collection, use, storage, and disclosure practices. This plan also includes "Breach Detection Process" which is listed as an ongoing task item. 1.c. Met with Chief Counsel for Technology and Business Services and noted he receives a series of monthly reports containing any unauthorized disclosures (including Covered Information) from the Cybersecurity Group. He identifies and tracks any unauthorized disclosures to be included in SoCalGas *Annual Privacy Report*.	
2. Assess whether SoCalGas filed its Annual Report to the CPUC as required by the Privacy Decision.	2.a. Reviewed SoCalGas' *2020 Annual Privacy Report* and noted it was submitted to the CPUC on April 30, 2021. The report identified 31 breaches within the 2020 calendar year.	

CPUC RULE 9 Accountability and Auditing

Overall assessment result	**Exception Noted:** SoCalGas has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas has a process in place to provide the Commission with the *Annual Privacy Report* or any other requested documentation	1.a. SoCalGas made available for this assessment the following documents, in line with the CPUC requirements: — *Privacy Notice* and *Privacy Policy* provided to customers and made available to the public through SoCalGas website — Internal privacy and data security policies — Listing of agents, contractors, and third parties with access to Covered Information — Templates of secondary-use authorization form (*CISR* form) by which SoCalGas secures customer authorization for Covered Information	

Assessment procedures	Assessment test results	Exceptions
	— Procedures for processes related to accessing, collecting, using, and disclosing Covered Information 1.b. Reviewed SoCalGas' *Customer Privacy Compliance Plan* which tracks the different business units responsible for the sections in the *Annual Privacy Report* as required by the CPUC. In addition, the document monitors compliance with sections of the *CPUC Privacy Decision*. SoCalGas' Privacy Team is responsible for working with the appropriate business units within the Company to complete the *Annual Privacy Report* and submit it to the CPUC. 1.c. Met with Senior Counsel of Regulatory Law and two Regulatory Case Managers and noted the process for compiling the *Annual Privacy Report* begins around February/March. A member of the Privacy Team compiles the report by gathering required information from all necessary business units. Multiple levels of review occur, including by the Privacy Team, Regulatory Team, multiple business units, and Legal. 1.d. Reviewed *2020 SoCalGas CPUC Annual Privacy Report: Schedule/Plan* and noted SoCalGas follows a schedule to file the *Annual Privacy Report* by the due date as required by the Commission.	

CPUC Rule 9	Rule description	**Customer complaints:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas provides notice to its customers on how the customers can contact the Company for inquiries, complaints or disputes related to their personal information.	1.a. Reviewed SoCalGas' *Privacy Notice* and noted customers can limit, view, or dispute their disclosed information by contacting SoCalGas via email, through mail to the Customer Privacy Program Manager, or by phone. 1.b. Met with representatives from SoCalGas' Customer Contact Centers and was informed customers could contact SoCalGas' Customer Contact Center or email inquiries to inquire, complain, or dispute issues related to their personal information. 1.c. Reviewed SoCalGas website and observed SoCalGas provides multiple telephone numbers (including numbers for multilingual customer service), a postal mailing address, and a link to find a payment location near the customer under "Contact US." 1.d. Observed *Annual Privacy Notice Bill Insert* and noted SoCalGas provides existing customers a bill insert encouraging customers to review the *Privacy Notice* on an annual basis. 1.e. Met with Branch Office Manager and two Branch Office Supervisors during the walk-through of the Santa Ana Branch Office and noted customers can go to a Branch Office to inquire about their account.	
2. Assess whether SoCalGas 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 SoCalGas' *Customer Contact Operating Procedures- Customer Comment Tracking System* and noted the document outlines the process to receive and address customer complaints for resolution. Customer compliments, comments, and complaints are tracked within the comment tracking system. Customer comments are organized into urgent, high, and low priority and dealt with according to each priority's procedures. 2.b. Reviewed the *Bill Investigation Procedure* addressing the procedures CSSs follow when a customer has questions about or disagrees with their bill amount.	

Assessment procedures	Assessment test results	Exceptions
	2.c. Reviewed *Customer Complaint Elevation Guidelines* and *Referral Chart for Elevated Written Complaints* and noted SoCalGas provides their employees with escalation guidelines for when written and phone complaints require further assistance for resolution. 2.d. Reviewed *Residential Marketing Support Center (RMSC) Procedure - Reporting My Account and Breach Issues* and noted the procedures Residential Marketing team follows regarding privacy-related complaints. 2.e. Inspected a sample *Customer Complaint* and noted the workflow followed SoCalGas procedures for documenting, classifying, and resolving customer complaints.	
3. Assess whether SoCalGas has a process to escalate disputes, complaints, and inquiries to help ensure resolution within a timely manner.	3.a. Met with members of the Customer Contact Center and was informed if a customer called in a complaint related to customer privacy, it would be routed to Residential Marketing, who would then review it and if necessary escalated to (i) Information Security (Corporate Security) or (ii) the Privacy Office for resolution, depending on the specific content of the complaint. Complaints are tracked through SoCalGas Customer Comment Tracking System and a report is generated monthly containing outstanding unresolved complaints. 3.b. Reviewed *Customer Contact Operating Procedures - Customer Comment Tracking System* and noted CSR Leads are automatically alerted when disputes, complaints, or inquiries are classified as "Urgent" in the comment tracking system. These situations require immediate action, while "High" priority complaints require action on the same day or next morning. 3.c. Met with Executive Special Investigations Case Managers, who resolve complaints filed with the CPUC, and was informed customers can file an informal complaint with the CPUC regarding SoCalGas. Once filed, members of the Investigations Case Team have 30 days to respond in writing to the customer and the CPUC.	
4. Inspect evidence that SoCalGas tracks and resolves customer complaints consistent with SoCalGas' policies.	4.a. Inspected *SoCalGas CPUC Customer Complaints Report* and noted SoCalGas categorizes and tracks the number of executive, informal, telephone, and formal complaints received from customers. Complaints	

Assessment procedures	Assessment test results	Exceptions
	were most often related to high bills and inquiries in miscellaneous categories. 4.b. Met with Executive Special Investigations Case Managers and was informed there were no CPUC Complaints for 2021 specifically associated to customer data privacy and security concerns.	

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

Assessment procedures	Assessment test results	Exceptions
1. Review SoCalGas' documented privacy awareness program materials to identify personnel who handle and access Covered Information.	1.a. Met with members of the Privacy Team, Regulatory Compliance Advisor, and member of the Cybersecurity Team and was informed all SoCalGas employees are required to complete two trainings that include sections regarding Covered Information. In addition, each business unit is assigned a "Privacy Pro" required to complete an additional training with supplementary privacy content. 1.b. Met with members of the Privacy Team and learned that once a year, the Privacy Team works with IT to pull a listing of contractors with access to systems containing Covered Information. The Privacy Team also reaches out to the managers of these contractors to ensure the contractors have access to and handle Covered Information. Contractors included in the resulting population are assigned SoCalGas' *Customer Data Privacy Training*. 1.c. Met with members of the Mass Market Credit and Collections Team and noted completion of a yearly *FACTA Training* which includes content on personally identifiable information is mandatory trainings for all department employees.	SoCalGas has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.
2. Understand the awareness material and communications to SoCalGas personnel to test how internal privacy policies are communicated to associates.	2.a. Met with members of the Privacy Team and was informed internal privacy policies were communicated to SoCalGas employees and contractors through the following trainings: — All SoCalGas employees are assigned and required to complete the *Cybersecurity Training* with a *Privacy Module* on an annual basis. New hires are required to complete these trainings upon onboarding. — All SoCalGas employees along with contractors who have access to Covered Information are required to complete SoCalGas *Customer Data Privacy Training*. — Each department is assigned a "Privacy Pro" who is required to complete the *Privacy Pro Training,* with detailed privacy content.	

Assessment procedures	Assessment test results	Exceptions
	2.b. Reviewed additional privacy awareness documents and communications related to customer privacy, including the following: — Messages from the CIO regarding Cybersecurity Awareness — Emails sent out to employees containing phishing and data privacy content — Intelligence reports posted on SoCalGas privacy intranet site covering various cyber topics 2.c. Reviewed SoCalGas' *New Hire Welcome Package* and noted the following documents are mailed to new employees: — *Employee Standards of Conduct* — *Confidential Information and Invention Assignment Agreement* — The *Cybersecurity Training* with a *Privacy Module* and *Customer Data Privacy Training* are also required to be completed by all new employees 2.d. Met with members of the Customer Operations Team and noted a Privacy Pro is assigned to every business unit and are required to attend privacy-related meetings. At each meeting, Privacy Pros are presented with information to share with their respective business units. 2.e. Reviewed SoCalGas privacy intranet accessible by all employees, which contains links to internal privacy resources, trainings, steps to report security incidents, and other data protection resources. 2.f. Reviewed SoCalGas *Telework for Exempt Employees* document signed by employees working remotely due to COVID-19. The agreement includes SoCalGas clean desk policy, information and physical security rules, and emphasizes all company policies are applicable while working remotely. 2.g. Reviewed sample *Work from Home Agreement* signed by CSSs working remotely. Noted the agreement outlines the eligibility to work from home and expectations to maintain such eligibility. The agreement also mentions that all company policies and employee responsibilities are still applicable.	

Assessment procedures	Assessment test results	Exceptions
3. Understand SoCalGas' 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 the enterprise-wide *Cybersecurity Training* which includes a privacy module and noted every SoCalGas employee is required to complete this training. The training consists of a video and quiz at the end. This training provides examples of customer information (including PII and Covered Information) and provides guidelines for the collection, storing, sharing, and disposal of customer data. Employees must pass the quiz at the end to receive completion credit. 3.b. Reviewed *Customer Data Privacy Training* mandatory for employees and contractors with access to Covered Information and noted the training is a PowerPoint discussing personal, sensitive, and Covered Information. Once completed, employees and contractors must mark it "completed" and acknowledge they understand the content and have completed the training. 3.c. Reviewed *Privacy Pro Training* and noted it provides Privacy Pros with knowledge regarding personal and Covered Information and also requires Privacy Pros to complete a personal information certification. 3.d. Met with members of the Privacy Team, Regulatory Compliance Advisor, and member of the Cybersecurity Team and was informed the Learning Management System tracks employee training completion. Employees receive automated email reminders to complete their required trainings. Once an employee is past 14 days due, their manager receives an email. If the training is still not completed, the director is notified. 3.e. Reviewed multiple training tracking compliance logs and noted SoCalGas' Privacy Department tracks completeness of required privacy related trainings. 3.f. Inspected *Cybersecurity Training Tracker* and noted at the end of 2021, 98.54% of SoCalGas employees had completed the *Cybersecurity Training with the Privacy Module*.	
4. Inspect evidence that contractors have completed privacy and security training requirements (e.g., training logs, certifications of compliance, etc.).	4.a. Met with members of the Privacy Team, Regulatory Compliance Advisor, and member of the Cybersecurity Team and was informed contractors are under contractual obligation to follow SoCalGas data privacy rules. KPMG was also informed manual emails were sent out on multiple	

Assessment procedures	Assessment test results	Exceptions
	instances to contractors to enforce completion of the *Customer Data Privacy Training*. 4.b. Inspected *Customer Data Privacy Training Tracker* for contractors and noted 91% of contractors had completed the required training.	
5. Understand the privacy training required of third parties accessing Covered Information in order to test whether or not they are adequately equipped to handle Covered Information.	5.a. Met with members of the Privacy Team, Regulatory Compliance Advisor, and member of the Cybersecurity Team and was informed vendor contracts have explicit and thorough language to ensure contractors abide by corporate rules regarding data privacy and security. Contractors are contractually obligated to follow all SoCalGas privacy rules. 5.b. Reviewed Sempra's *Supplier Code of Conduct* provided to contractors and noted policies regarding information protection and confidentiality: — Nonpublic information contained in electronic or physical form must be appropriately secured and protected. — Nonpublic information accessed by suppliers must be limited to only that information that is required to perform the contracted work. — If suppliers are granted access through electronic or physical means to Sempra Energy's nonpublic information to perform Sempra Energy-related work, the information may only be used for Sempra Energy business. — Suppliers must keep nonpublic information confidential and may only disclose non-public information if it is necessary for the performance of their work. Such disclosures may be made only to those people who are also subject to Sempra Energy's confidentiality provisions and have a legitimate business need to know. 5.c. Inspected a sample NDA and a sample MSA between SoCalGas and a supplier with access to Covered Information and noted both contracts included confidentiality and non-disclosure clauses containing a definition of confidential information, governance regarding the handling of customer information, and consequences for noncompliance. 5.d. Inspected a sample of executed vendor contracts and noted they include confidentiality clauses protecting SoCalGas' confidential information. The	

Assessment procedures	Assessment test results	Exceptions
	contracts also state the contractor may be required to complete training at SoCalGas' sole discretion.	

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 noncompliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each noncompliance and a detailed description of each noncompliance.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SoCalGas tracks the reporting requirements and assigns responsibility and accountability to the appropriate departments.	1.a. See CPUC Rule 9a (1) for test results. 1.b. Reviewed SoCalGas' *Customer Privacy Compliance Plan* and noted the Privacy Team is responsible for working with the appropriate business units within the Company to complete the *Annual Privacy Report* and submit it on time to the CPUC. This document also tracks the different business units responsible for information required to be included in the *Annual Privacy Report*. 1.c. Reviewed *2020 SoCalGas CPUC Annual Privacy Report: Schedule/Plan* and noted SoCalGas follows a schedule to ensure the *Annual Privacy Report* is submitted to the CPUC by the due date enforced by the Commission.	
2. Assess whether SoCalGas filed its Annual Report to the CPUC as required by the Privacy Decision.	2.a. Reviewed SoCalGas' *2020 Annual Privacy Report* and noted it was submitted to the CPUC on April 30, 2021, and included: — The number of unique authorized third parties accessing Covered Information — The number of noncompliances with CPUC privacy rules or with contractual provisions required by the Privacy Rules known to SoCalGas 2.b. The number of customers affected by each noncompliance and a description of each noncompliance	

Appendix II - Abbreviations used in this report

Abbreviation	Full name
CCPA	California Consumer Privacy Act
CEUD	Customer Energy Usage Data
CIS	Customer Information System
CISR	Customer Information Service Request
CPUC	California Public Utilities Commission
CEC	Cybersecurity Engineering Risk and Consulting
CSR	Customer Service Representatives
CSS	Customer Service Specialists
DLP	Data Loss Prevention
DMZ	Demilitarized Zone

Abbreviation	Full name
EDRP	Energy Data Request Program
ERIM	Enterprise Records and Information Management
GAPP	Generally Accepted Privacy Principles
GRC	Governance Risk & Compliance
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
IS	Information Security
ISO	International Organization for Standardization
IT	Information Technology
IT PMO	Information Technology Portfolio Management Office
ITVMO	Information Technology Vendor Management Office
LOB	Line of Business
MSA	Master Service Agreement
NDA	Non-Disclosure Agreement
PIA	Privacy Impact Assessment

Abbreviation	Full name
PII	Personally Identifiable Information
QA	Quality Assurance
RMSC	Residential Marketing Support Center
SCG	Southern California Gas Company
SDLC	Software/System Development Life Cycle
SIEM	Security Information and Event Management

Appendix III - Stakeholders interviewed

#	Title	Organizational Unit	Date
1	Customer Services Technology Manager	Customer Operations	11/2/2021
2	Customer Operations Privacy Program Manager	Customer Operations	11/2/2021
3	Project Manager - II - EC – PT	Customer Operations	11/2/2021
4	Business Systems Analyst	Customer Operations	11/2/2021
5	Project Advisor- Special Projects/PMO	Customer Operations	11/2/2021
6	Customer Services Technology Manager	Customer Operations	11/3/2021
7	Project Manager – II	Customer Services	11/12/2021
8	QA & Analytics Manager	Audit Services	11/12/2021
9	IT Auditor	Audit Services	11/12/2021
10	Audit Services Manager	Audit Services	11/12/2021

#	Title	Organizational Unit	Date
11	Value Capability Manager	Cybersecurity Risk & Compliance	11/15/2021
12	Domain Engineer - Cyber	Cybersecurity Risk & Compliance	11/15/2021
13	Software Developer Manager	Systems & Technology - Customer	11/16/2021
14	Customer Contact Center Operations Support Manager	Customer Contact Centers	11/17/2021
15	Customer Services Technology Advisor	Customer Contact Centers	11/17/2021
16	Executive Special Investigations Case Manager	Customer Contact Centers	11/17/2021
17	Customer Services Technology Advisor	Customer Contact Centers	11/17/2021
18	Executive Special Investigations Case Manager	Customer Contact Centers	11/17/2021
19	Strategy & Operations Manager	Digital Enablement Services	11/17/2021
20	Director – Cybersecurity Risk & Compliance	Cybersecurity Risk & Compliance	11/17/2021
21	Senior Paralegal	Litigation	11/18/2021
22	Senior Counsel	Litigation	11/18/2021
23	Customer Contact Center Site Manager	Customer Contact Centers	11/19/2021
24	Factory Manager II	Support Services	11/19/2021
25	Customer Contact Center Supervisor	Customer Contact Centers	11/19/2021
26	Customer Contact Center Supervisor	Customer Contact Centers	11/19/2021
27	Security Manager	Corporate Security	12/1/2021

#	Title	Organizational Unit	Date
28	Director	Corporate Security	12/1/2021
29	Manager	Compliance & Risk	12/1/2021
30	Physical Security Operations Advisor	Security, Compliance & Executive Services	12/1/2021
31	Billing Manager	Customer Operations	12/2/2021
32	Project Manager – II	Customer Operations	12/2/2021
33	Mass Market Credit & Collections Manager	Customer Operations	12/3/2021
34	Project Manager – I	Customer Operations	12/3/2021
35	Demand Response Manager	Customer Programs	12/6/2021
36	Senior Group Product Manager	Cloud & Infrastructure	12/7/2021
37	Group Product Manager	Cloud & Infrastructure	12/7/2021
38	Domain Architect – Cybersecurity	Cybersecurity Risk & Compliance	12/7/2021
39	Chief Counsel Technology & Business Services	Technology & Business Services	12/8/2021
40	Regulatory Compliance Advisor	Enterprise Risk & Compliance	12/9/2021
41	Regulatory Affiliate Compliance Manager	Risk & Compliance	12/9/2021
42	Regulatory Compliance Analyst	Risk & Compliance	12/9/2021
43	Director - Digital & Customer	Digital & Consumer	12/10/2021
44	Senior Counsel	General Counsel - Regulatory	12/13/2021
45	Regulatory Case Manager – III	CPUC/FERC - Gas	12/13/2021

#	Title	Organizational Unit	Date
46	Regulatory Case Manager – II	CPUC/FERC - Gas	12/13/2021
47	Senior Counsel	Regulatory	12/13/2021
48	Regulatory Business Manager	Policy & Proceedings	12/13/2021
49	Portfolio Manager	Supply Management & Div Business Enterprise	12/13/2021
50	Value Capability Manager	Cybersecurity Risk & Compliance	12/13/2021
51	Project Advisor - Special Projects/PMO	Customer Operations	12/14/2021
52	Domain Engineer Tm Ld- Cyber	Cybersecurity Risk & Compliance	12/14/2021
53	Director - Cloud & Infrastructure	Cloud & Infrastructure	12/15/2021
54	Senior Privacy Standards Advisor	Customer Operations	12/15/2021
55	Principal Special Agent	Corporate Security	12/15/2021
56	Factory Manager	Support Services	12/15/2021
57	Senior Domain Architect	Digital Workspace & Automation	12/15/2021
58	Security Manager	Corporate Security	12/15/2021
59	Customer Services Technology Advisor	Customer Contact Centers	12/16/2021
60	Project Manager (NSA)	Customer Operations	12/16/2021
61	Value Capability Manager	Cyber Security Operations	12/17/2021
62	IAM Manager	Digital Workspace & Automation	1/7/2022

#	Title	Organizational Unit	Date
63	IAM Manager	Digital Workspace & Automation	1/7/2022
64	Senior Domain Architect	Digital Workspace & Automation	1/7/2022
65	Branch Ofc Manager	Remittance Processing	1/11/2022
66	Project Manager – II	Remittance Processing	1/11/2022
67	Regulatory Branch Ofc Supervisor	Remittance Processing	1/11/2022
68	Branch Ofc Supervisor	Remittance Processing	1/11/2022
69	Branch Ofc Supervisor	Remittance Processing	1/11/2022
70	Customer Services Technology Advisor	Remittance Processing	1/11/2022
71	Director Customer Operations	Customer Operations	1/13/2022
72	Senior Vice President, Chief Information Office, and Chief Digital Officer	Senior Vice President, Chief Information Office, and Chief Digital Officer (Executive Offices)	2/2/2022

Contact us

Doron Rotman
Managing Director
408-367-7607
drotman@kpmg.com

Alicia Ortego
Director
415-260-5828
aortego@kpmg.com

Chris Kypreos
Director
415-963-5148
ckypreos@kpmg.com

www.kpmg.com

kpmg.com/socialmedia

APPENDIX C

SDG&E Covered Information Privacy and Security Assessment Report

San Diego Gas and Electric Company

CPUC Covered Information Privacy and Security Assessment Report

For the period January 1, 2021
through December 31, 2021

February 25, 2022

kpmg.com

Contents

Document structure

This report consists of the following sections:

Executive summary – an overview of the project including background, scope, and KPMG's overall results and noted exceptions and recommendations, where necessary, for each Rule comprising the *California Public Utility Commission Privacy Decision*.

Project approach and methodology – an overview of key project phases and activities performed by KPMG throughout the course of the assessment.

Rule assessment results, exceptions, and recommendations – a summary of KPMG's assessment associated with each of the nine (9) Rules of the *CPUC Privacy Decision* including KPMG's interviews and document reviews (e.g., test work), overall results, detailed exceptions, and improvement recommendations associated with each exception.

SDG&E's Management Response to CPUC Covered Information Privacy and Security Assessment Report – SDG&E's Management Response to the *CPUC Covered Information Privacy and Security Assessment Report* dated February 25, 2022.

Appendix I – Detailed assessment procedures and results – the full details of KPMG's assessment criteria, procedures, and results for each Rule.

Appendix II – Abbreviations used in this report – a list of the abbreviations and acronyms used throughout this Report.

Appendix III – Stakeholders interviewed – a list of each stakeholder interviewed by KPMG throughout the course of the assessment.

Executive summary

Through its Smart Meter and meter-to-cash operations, San Diego Gas and Electric Co. (hereinafter "SDG&E," the "Utility," or "Company") collects, processes, stores, and discloses Customer Energy Usage Data (CEUD) and other Customer Personally Identifiable Information (PII). The PII contains names, addresses, Social Security Numbers (SSNs), service account numbers, and financial account information. When combined, CEUD and PII represent Covered Information.

Background

On July 28, 2011, the California Public Utilities Commission (CPUC) issued Decision D.11-07-056 "Rules Regarding Privacy and Security Protections for Energy Usage Data" and Decision D.14-12-004 "Decision Extending Privacy Protections to Customers of Gas Corporations and Community Choice Aggregators and to Residential and Small Commercial Customers of Electric Service Providers" (hereinafter the "*Privacy Decisions*"). The *Privacy Decisions* requires SDG&E to undergo an independent assessment of its Covered Information privacy and security practices. Covered Information is defined in the *Privacy Decisions* as CEUD obtained via Advanced Metering Infrastructure combined with other information that could reasonably be used to identify a residential customer, family, household, residence, or nonresidential customer. Covered Information does not include information provided to the CPUC pursuant to its oversight responsibilities.

SDG&E engaged KPMG to conduct an independent assessment of the Company's Covered Information privacy and security processes, controls, and practices in conjunction with general rate case proceedings.[1] This report represents the results of KPMG's assessment.

Prior to the period under review, the US Department of Health and Human Services declared a national health emergency due to the COVID-19 pandemic. As a result, the State of California declared a State of Emergency and executed a stay-at-home order causing the majority of SDG&E's workforce to migrate to a remote working environment. SDG&E adapted and adjusted several of its safeguards and processes over Covered Information in light of the new remote working environment impacting the vast majority of the workforce. This remote working environment remained in effect during the covered period (2021), KPMG's team also adjusted its approach to deliver the assessment by using various forms of media, technology, and a virtual team infrastructure to execute this assessment 100% remotely.

[1] Independent privacy and security practices assessment is not intended to be an audit, examination, attestation, special report or agreed-upon procedures engagement as those services are defined in American Institute of Certified Public Accountants literature applicable to such engagements. Accordingly, these services will not result in the issuance of a written communication to third parties by KPMG directly reporting on financial data or internal control or expressing a conclusion, an opinion, or any other form of assurance.

Scope

The scope of KPMG's assessment was limited to systems and Lines of Business (LOBs) collecting, processing, storing, or disclosing Covered Information. The scope does not cover an assessment of SDG&E's practices, procedures, and controls to safeguard employee or contractor PII, or other customer PII that is not Covered Information.

To perform the review, KPMG used an Assessment Framework comprised of multiple criteria based on various industry leading standards. KPMG mapped the Assessment Framework criteria to the nine (9) Rules in the *Privacy Decision* and used the framework to perform the assessment of SDG&E's privacy and security practices, procedures, and controls to safeguard Covered Information.

— The *Covered Information Privacy and Security Practices Assessment* was based on KPMG's review and understanding of the practices, procedures, and controls in place from **January 1, 2021 through December 31, 2021** (the Covered Period).

— The exceptions and recommendations were based on KPMG's review of policy/procedure documents, stakeholder interviews, inspection of sample communications to customers and third parties, Covered Information access reports, system security profiles, and virtual site walk-throughs.

— In typical years, KPMG would perform physical site walk-throughs to observe physical, technical, and administrative privacy and security controls implemented where Covered Information is collected, stored, and processed. However, as a result of the global pandemic, KPMG was unable to conduct physical site walk-throughs as part of the 2021 assessment. KPMG did conduct virtual site walkthroughs of a Contact Center, Billing and Processing Center, Sempra Production Data Center, and a Branch Office. KPMG's observations are limited to observations identified through such virtual site walk-throughs, stakeholder interviews, virtual screen sharing and documentation reviews.

— KPMG conducted 40 interviews with personnel from various LOBs including Audit Services, Cloud & Infrastructure, Corporate Security, CPUC/FERC – Gas, Customer Care, Customer Field Operations, Customer Operations, Customer Services & External Affairs, Cybersecurity Risk & Compliance, Digital & SDGE Customer, Digital Enablement Services, Digital Workspace & Automation, Enterprise Risk & Compliance, Gas Engineering, General Counsel- Regulatory, Litigation and Wildfire Mitigation, Policy & Proceedings, Regulatory, Risk & Compliance, Security Compliance & Executive Services, Supply Management & Div Business Enterprise, Support Services- SDG&E, and Technology & Business Services. KPMG also conducted interviews with SDG&E's privacy and security executives to understand general Covered Information oversight, management, and tone at the top.

— KPMG assessed the design and implementation of privacy and security controls followed by an assessment of operating effectiveness of key implemented controls.

The nine (9) Rules noted in the *Privacy Decision* 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

Summary of exceptions

KPMG has noted **6** Exceptions (Exceptions are areas where SDG&E's program may not be fully prepared to meet compliance with CPUC *Privacy Decision* requirements, as measured against KPMG's Assessment Framework, developed to test controls around Covered Information identified in the rules). The Exceptions are shown below along with the recommendations associated with each Exception. There were **3** Low-Risk Exceptions, **3** Medium-Risk Exceptions, and **0** High-Risk Exceptions. The risk rating methodology is based on the following definitions:

Risk level	Description
High	Issue poses a significant risk of data breach of Covered Information and/or a significant deviation from the *CPUC Privacy Decision*.
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 Decision*.
Low	Procedures or practices supporting the protection of Covered Information and alignment with the *CPUC Privacy Decision* may not be formally defined or documented.

For more details associated with each Rule, see **Rule assessment results, exceptions, and recommendations**, and **Appendix I – Detailed assessment procedures and results**.

CPUC rule number	Risk level	Exceptions noted	KPMG recommendations
CPUC Rule 1 Definitions	-	-	N/A
CPUC Rule 2 Transparency (Notice)	**Low**	New SDG&E Customers are not being provided written notice regarding the accessing, collection, storage, use, and disclosure of Covered Information upon registering a new account. New customers receive a confirmation email upon registration which contains a link to the *Privacy Notice*. While this link is also a requirement under Rule 2b (and should be included on all electronic correspondence to customers), it does not replace the requirement to provide a written notice when confirming a new customer account. Customers that receive a paper monthly statement	Management should consider providing customers with SDG&E's *Privacy Notice* upon registering a new account. For paperless customers, this may be in the form of an email containing an attachment with SDG&E's *Privacy Notice* and for non-paperless customers, this could be an additional flier sent out after the customer registers a new account.

		are provided the *Privacy Notice* as an insert in their first bill. Customers that have opted for paperless billing receive an email with a link to a site where all inserts for the month may be viewed.	
CPUC Rule 3 Purpose Specification	**Low**	SDG&E's *Privacy Notice* provided to customers states that the customer may contact SDG&E if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.	Management should consider updating SDG&E's *Privacy Notice* to include the consequences customers may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.
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**	Current SDG&E standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, KPMG observed inconsistent or missing privacy and security provisions in several sampled vendor contracts, which do not align to formal regulatory requirements.	Management should consider reviewing third-party contracts involving sharing Covered Information and ensure the contracts include the required standard language to enhance customer privacy protection and help ensure Covered Information is properly managed by third parties.
CPUC Rule 7 Data Quality and Integrity	-	-	N/A
CPUC Rule 8 Data Security	**Medium**	One SDG&E application storing Covered Information did not meet the baseline Sempra security requirements for	Management should consider implementing the baseline Sempra Cybersecurity control requirements to adequately

		user authentication and audit logging during the covered period.	protect Covered Information stored and processed within the application.
CPUC Rule 9 Accountability and Auditing	**Low**	SDG&E has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their on-boarding. This will help to ensure contractors are properly trained in a timely manner on how to access, collect, store, use, and disclose Covered Information.
	Medium	SDG&E has a process in place to identify contractors with access to Covered Information and to assign relevant trainings regarding how to use, store, or process Covered Information. However, SDG&E is unable to enforce contractor trainings and therefore, completion rates could be lower than deemed reasonable.	Management should consider implementing a process to enforce contractor training completion. This could include follow-up emails, as well as escalation procedures (e.g., management involvement or termination of access to SDG&E systems) for contractors who have not completed the training in a timely manner.

Project approach and methodology

KPMG approached the Assessment in four (4) phases: Mobilize, Assess, Validate, and Report.

— **Mobilize –** KPMG validated the Assessment Framework used to review SDG&E's privacy and security practices based on the nine (9) Rules comprising the *Privacy Decision*. KPMG created this framework at the inception of the *Privacy Decision*, and it has been used across all the California IOUs. The framework has evolved overtime to reflect changes in the environment, market expectations and Utilities maturing programs.

  KPMG worked with SDG&E's Privacy team to identify relevant stakeholders, reviewed the organizational structure to identify business groups where Covered Information may reside, reviewed the current IT landscape to identify systems and applications that collect, store, or process Covered Information, and documented existing system profiles for systems and applications that collect, store and process Covered Information.

— **Assess –** As part of the assessment, KPMG performed a variety of interviews with stakeholders representing various LOBs. KPMG interviewed a unique total number of **76** personnel in a total of **40** interviews, submitted **226** document requests, reviewed approximately **300** documents and **43** system assessments, and performed **4** virtual site walk-throughs of critical SDG&E facilities (Customer Contact Center, Data Center, Credit and Billing Center, and Branch Office) to observe safeguards in place to protect Covered Information.

— **Validate –** KPMG validated draft observations throughout the Assessment phases with the SDG&E Privacy team, relevant IT and business stakeholders, and SDG&E leadership.

— **Report –** KPMG developed a final report providing exceptions and recommendations and incorporated SDG&E's Management Response to the validated Exceptions.

Rule assessment results, exceptions, and recommendations

For each identified Exception, KPMG reviewed the risk and assigned a risk rating of **High, Medium,** or **Low** based on the potential impact the Exception could have as it relates to the protection of Covered Information. The risk rating methodology used the following definitions:

Risk level	Description
High	Issue poses a significant risk of data breach of Covered Information and/or a significant deviation from the *CPUC Privacy Decision*.
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 Decision*.
Low	Procedures or practices supporting the protection of Covered Information and alignment with the *CPUC Privacy Decision* are not formally defined or documented.

KPMG noted **6** specific Exceptions, comprised of **3** Low-Risk Exceptions, **3** Medium-Risk Exceptions, and **0** High-Risk Exceptions. The Exceptions identify areas where SDG&E's program is not fully prepared to meet requirements under the *Privacy Decision*.

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

Rule 2: Transparency Notice

KPMG assessment procedures	KPMG assessed SDG&E's overall customer notice program focusing on: — Review internal and customer-facing *Privacy Policies* and *Privacy Notice* that address SDG&E's practices and procedures related to the collection, processing, storage, and disclosure of Covered Information; — Interview with SDG&E Privacy Team personnel and review of methods and frequency for providing customers with the *Privacy Notice*; — Interview Energy Service Specialists (ESSs) to discuss interactions with customers and discussing their Covered Information.
Results summary	SDG&E provides its external-facing *Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information* (*Privacy Notice*) and *Privacy Policy* 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 a contact telephone number and mailing address where customers can contact SDG&E with complaints, inquiries, and disputes regarding their Covered Information and SDG&E's *Privacy Notice*. There is a "Privacy Center" link located at the bottom of SDG&E's homepage, which takes the customer to privacy related resources, including the *Privacy Notice*. SDG&E provides its *Privacy Notice* to new customers with their first bill, and annually thereafter in a bill insert. The *Privacy Notice* is available in 19 languages to accommodate SDG&E's largest customer demographics. SDG&E also makes available its previous versions of the *Privacy Notice* upon request. Customers can email privacy@sdge.com or contact the Office of Customer Privacy (OCP) to request prior versions of SDG&E's *Privacy Notice*.
Exception	New SDG&E Customers are not being provided written notice regarding the accessing, collection, storage, use, and disclosure of Covered Information upon registering a new account. New customers receive a confirmation email upon registration which contains a link to the *Privacy Notice*. While this link is also a requirement under Rule 2b (and should be included on all electronic correspondence to customers), it does not replace the requirement to provide a written notice when confirming a new customer account. Customers that receive a paper monthly statement are provided the *Privacy Notice* as an insert in their first bill. Customers that have opted for paperless billing receive an email with a link to a site where all inserts for the month may be viewed.
Risk level	**Low**
Risk implication	Per CPUC *Privacy Decisions*, customers must be provided written notice upon registration for a new account to be aware of the Utility's privacy practices.

Recommendation	Management should consider providing customers with SDG&E's *Privacy Notice* upon registering a new account. For paperless customers, this may be in the form of an email containing an attachment with SDG&E's *Privacy Notice* and for non-paperless customers, this could be an additional flier sent out after the customer registers a new account.

Rule 3: Purpose Specification

KPMG assessment procedures	KPMG assessed SDG&E's specification of the purposes focusing on: — Review how SDG&E specifies the reasons for which it collects, discloses, retains, and provides access to Covered Information; — Review of SDG&E's *Privacy Notice*, as well as other policies and procedures; — Interview stakeholders to understand the determination and specification of information and third-party categories; — Examine whether the *Privacy Notice* includes a description of how customers can access and control their Covered Information collected, processed, stored, and disclosed by SDG&E; — Interview SDG&E personnel on procedures to assist customers with accessing, inquire about, or dispute their covered information.
Results summary	SDG&E has documented policies and procedures outlining the acceptable purposes for which Covered Information may be collected, stored, used, and shared. These include detailed policies regarding disclosure of Covered Information for both primary and secondary purposes. In addition, the *Privacy Notice* includes ways the Customer can contact SDG&E to limit the collection, use, and storage of Covered Information. Per Company policy, Covered Information is not disclosed for secondary purposes, without customer authorization. SDG&E's *Privacy Notice* includes the categories of third parties SDG&E may share Covered Information with, and circumstances under which that information may be shared. SDG&E has implemented internal policies, procedures, and standards instructing employees on determining the veracity and propriety of third-party requests for customer information, the relevant customer consent forms, and on the appropriate use of Covered Information.
Exception	SDG&E's *Privacy Notice* provided to customers states that the customer may contact SDG&E if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.
Risk level	**Low**
Risk implication	Per CPUC *Privacy Decision*, customers must be informed of the consequences associated with limiting their Covered Information in order to be able to make informed decisions related to their information.
Recommendation	Management should consider updating SDG&E's *Privacy Notice* to include the consequences customers may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.

Rule 4: Individual Participation (Access and Choice)

KPMG assessment procedures	KPMG assessed SDG&E's customer-facing program focusing on: — Review internal and external policies and procedures to provide customers with access and consent mechanisms related to their Covered Information; — Review customer portals, perform stakeholder interviews, and conduct virtual walk-throughs of the Customer Contact Center and Branch Offices where SDG&E ESSs interact with customers with respect to their Covered Information; — Review customer authorization forms to understand how customers can grant and revoke authorization of their Covered Information for secondary purposes; — Examine 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.
Results summary	SDG&E provides customers with multiple methods to access their Covered Information, including notifications on their monthly bills, via SDG&E's *MyAccount* portal and *Energy Usage Reports* that allow them to review and interpret their CEUD. Customers may contact SDG&E through phone, web, email, or mail with questions or concerns regarding their Covered Information, account, and monthly bills. SDG&E ESSs authenticate customers and validate their account information when answering calls prior to addressing customers' questions or concerns. Internal guidelines for SDG&E employees who interact with customers are in place and address how to provide customers with access to their Covered Information. SDG&E has processes and procedures in place for customers to grant and revoke authorization to third parties through the use of the *Customer Information Service Request (CISR)* form. Customer-facing policies and notices indicate SDG&E may disclose Covered Information if it is necessary to provide energy services, to comply with relevant laws, to respond to subpoenas or warrants, or to provide emergency responders with pertinent information in the case of imminent threat to life or property. Per SDG&E's *2020 Annual Privacy Report,* SDG&E received 416 demands to disclose Covered Information pursuant to legal processes and zero requests for Covered Information due to imminent threat to life or property.
Exception	No Exceptions noted
Risk level	-
Risk implication	-
Recommendation	-

Rule 5: Data Minimization

KPMG assessment procedures	KPMG assessed SDG&E's adoption of Data Minimization principles in the collection, use, and disclosure of Covered Information focusing on: — Review corporate and department-specific policies and procedures to understand how Covered Information is segregated from other systems; — Interview stakeholders to determine how user access to Covered Information is limited based on business need; — Examine how records and assets are retained for only as long as reasonably necessary; — Inspect the proper disposal of records upon their eligibility for disposition; — Interview stakeholders to determine how Data Minimization principles were adopted as part of third-party disclosure practices; — Perform virtual site walk-throughs at the Customer Contact Center, Branch Offices, and interviews with ESSs to understand how Data Minimization is implemented in the Contact Centers, Branch Offices, and in a remote working environment.
Results summary	SDG&E has implemented the Data Minimization principle as a foundational component to its overall privacy program framework. The company has documented policies and procedures limiting the amount of information collected, stored, and retained; the number and level of employees who have access to Covered Information; and the categories of third parties with whom it is shared. SDG&E enforces the same Data Minimization protocols within the Contact Centers and Branch Offices as they do for employees working remotely. Data Minimization is reinforced through various trainings and employee compliance with relevant policies and procedures is routinely reviewed. SDG&E management reviews and certifies that Covered Information is retained only as long as necessary for a specific business purpose and that it is properly disposed of in a timely manner.
Exception	No Exceptions noted.
Risk level	-
Risk implication	-
Recommendation	-

Rule 6: Use and Disclosure Limitation

KPMG assessment procedures	KPMG assessed SDG&E's Third-Party Management Program focusing on: — Examine processes in place for disclosure of Covered Information to third parties. "Third party" is defined to include suppliers and contractors; — Review procedures and forms for customers to authorize and revoke a third party to receive Covered Information on behalf of the customer; — Examine third-party management policies and procedures and interview of stakeholders to understand how SDG&E implements practices and procedures based on the categories of third parties; — Review third-party contract management process including onboarding, contract compliance reviews, and contract termination; — Review third-party (suppliers, vendors, contractors and consultants) risk management documentation; — Examine data transmission protocols and ongoing monitoring of third parties for compliance with SDG&E policies and contractual provisions.
Results summary	SDG&E has processes in place to allow customers to share their Covered Information with third parties. SDG&E has formal internal procedures to manage customer requests for disclosure to third parties, which include forms for explicit customer authorization and forms to revoke such authorization (*CISR* forms). Prior to providing services to SDG&E, all third parties must have a written formal agreement and must undergo a risk assessment conducted by the Information Technology Vendor Management Office (IT VMO). In addition, SDG&E has internal third-party management policies and informs third parties about data privacy requirements. Third-party vendors are contractually obligated to maintain the privacy of the information shared.
Exception	Current SDG&E standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, KPMG observed inconsistent or missing privacy and security provisions in several sampled vendor contracts, which do not align to formal regulatory requirements.
Risk level	**Medium**
Risk implication	Third-party vendors with access to Covered Information may have safeguards to protect customer privacy at levels less protective than those under which SDG&E operates.
Recommendation	Management should consider reviewing third-party contracts involving sharing Covered Information and ensure the contracts include the required standard language to enhance customer privacy protection and help ensure Covered Information is properly managed by third parties.

Rule 7: Data Quality and Integrity

KPMG assessment procedures	KPMG assessed SDG&E's data validation methods and procedures focusing on: — Interview stakeholders to determine how SDG&E validates the quality and integrity of Covered Information; — Examine the Smart Meter systems and infrastructure to understand how usage data is managed and reconciled; — Review policies and procedures and interviews with stakeholders to understand how SDG&E provides customers with the opportunity to modify or remove other data elements collected by the Company.
Results summary	SDG&E has policies in place that address the confirmation, validation, and relevance of customer information. The *Privacy Notice* provides customers with details to contact the Company by phone, email or mail should they need to view or dispute their information. In addition, Contact Center personnel authenticate and validate customer account information when answering a call. ESSs can assist customers with updating their information. SDG&E's *My Account Terms and Conditions* indicate it is the customers' responsibility to ensure their personal information is updated and accurate. System checks and manual processes are in place to validate energy usage reads and perform edits to help 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 assessment procedures	KPMG assessed SDG&E physical and Cybersecurity measures to protect Covered Information focusing on: — Review Cybersecurity policies, procedures, and measures related to: endpoint security (antivirus protection, email/database security), network security (network segmentation, Intrusion Prevention Systems/Intrusion Detection Systems, remote access, wireless, firewalls, network access controls), logging and monitoring, data loss prevention, web-content filtering, mobile security, vulnerability and patch management, business continuity/disaster recovery, change control (SDLC, cybersecurity assessments, privacy impact assessments, secure code reviews), access management (user provisioning and deprovisioning, access governance, privileged access, third-party access), and data classification; — Perform virtual site walk-throughs to observe and validate the physical and technical security controls implemented to safeguard Covered Information at the following critical SDG&E facilities: Customer Contact Center, a Branch Office, Production Data Center, Credit Operations and Billing Operations; — Inspect system profiles for in-scope systems storing Covered Information related to key configurations and system settings: System Access (user authentication and password configuration), Access Management (restriction of access based on least privilege and need-to-know, segregation of duties, periodic access reviews), Logging and Monitoring (system activity reviews, audit logs and audit trails of changes to customer data), Disaster Recovery, Data Protection (secure transfer mechanisms, encryption, masking of sensitive data); — Review the Sempra and SDG&E incident response and breach management program and interview stakeholders who are responsible and/or accountable in the response to a potential incident involving Covered Information, including communications to regulators and impacted customers; — Review evidence of tools deployed in the environment to detect and analyze potential threats to Covered Information.
Results summary	SDG&E has an established Information Security (IS) Program as part of Sempra shared services that is accountable and responsible for the design and implementation of both physical and logical information security controls to protect Covered Information. Formal policies and procedures have been established and implemented that address specific administrative, physical, and technical controls to protect Covered Information. Monitoring procedures are in place to detect and address noncompliance with policies and procedures. Various technical controls have been implemented to prevent and detect incidents and unauthorized access to systems containing Covered Information. A process is also in place to report and track potential security incidents and breaches to help ensure they are contained and eradicated, and measures are implemented to reduce the likelihood of similar events from occurring in the future.
Exception	One SDG&E application storing Covered Information did not meet the baseline Sempra security requirements for user authentication and audit logging during the covered period.

Risk level	**Medium**
Risk implication	Applications that do not meet Sempra's baseline Cybersecurity control requirements may result in the increased likelihood of unauthorized access and/or data leakage impacting the confidentiality, integrity, and availability of Covered Information.
Recommendation	Management should consider implementing the baseline Sempra Cybersecurity control requirements to adequately protect Covered Information stored and processed within the application.

Rule 9: Accountability and Auditing

KPMG assessment procedures	KPMG assessed SDG&E's overall Customer Data Privacy and Cybersecurity programs, focusing on: — Review documentation supporting each program as well as SDG&E's communication of these policies to both employees and contractors; — Interview stakeholders to understand the level of executive support and sponsorship of the Customer Privacy Program and Cybersecurity program, including the individuals and roles responsible and accountable for the customer privacy and cybersecurity throughout the Company; — Interview members of SDG&E's Executive Management to understand leadership's views on customer data protection; — Review processes to receive, track and resolve customer complaints, disputes, and inquiries related to the protection of Covered Information. Test procedures included a review of internal procedures, interviews with stakeholders involved in the complaints process, and virtual walk-throughs of the Customer Contact Center and Branch Offices; — Examine the employee and contractor training and awareness programs associated with the protection of Covered Information. This assessment included a review of enterprise-wide and targeted training materials provided to SDG&E employees and third-party contractors collecting, handling, storing, or transmitting Covered Information. Additionally, KPMG observed training compliance logs maintained for privacy trainings for employees and contractors.
Results summary	SDG&E has developed Company and department policies addressing proper safeguards of Covered Information. The Company has achieved a high level of maturity for its Customer Privacy Program, including a dedicated Customer Privacy Program Manager, who provides support, oversight, and visibility to reporting. Updates on data privacy and cybersecurity are regularly provided to management and the Board of Directors, and the Company's officers and directors reinforce the importance through awareness programs and town halls. A process exists to respond to complaints and inquiries levied by customers related to customer privacy. A Company-wide cybersecurity training and privacy training has been implemented and a targeted supplemental Customer Privacy training is provided to employees and contractors that have access to Covered Information.
Exception 1	SDG&E has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.
Risk level	**Low**
Risk implication	Contractors on-boarded after the annual launch of the training could use, process, or store Covered Information without being trained on how to handle Covered

	Information. In addition, a contractor could start and end their work assignment without being required to complete Covered Information training.
Recommendation	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their on-boarding. This will help to ensure contractors are properly trained in a timely manner on how to access, collect, store, use, and disclose Covered Information.
Exception 2	SDG&E has a process in place to identify contractors with access to Covered Information and to assign relevant trainings regarding how to use, store, or process Covered Information. However, SDG&E is unable to enforce contractor trainings and therefore, completion rates could be lower than deemed reasonable.
Risk level	**Medium**
Risk implication	Contractors with access to Covered Information could be on-boarded and off-boarded and never complete training on how to use, store, or process Covered Information.
Recommendation	Management should consider implementing a process to enforce contractor training completion. This could include follow-up emails, as well as escalation procedures (e.g. management involvement or termination of access to SDG&E systems) for contractors who have not completed the training in a timely manner.

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

February 25, 2022

Doron Rotman
Managing Director
KPMG LLP

Re: San Diego Gas & Electric Response to KPMG's 2021 Covered Information Privacy and Security Assessment Report

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 performing the 2021 SDG&E Covered Information Privacy and Security Assessment.

SDG&E engaged KPMG to perform this independent assessment to validate our company's compliance as required 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 reviewed the exceptions contained in KPMG's 2021 Covered Information Privacy and Security Assessment Report and provides the following attached response.

Sincerely,

Steve Rahon

Steve Rahon
Director, Customer Operations

Attachment

CPUC Rule Number	Risk Level	Exceptions Noted	KPMG Recommendation	SDG&E Management Response
CPUC Rule 1 Definitions	-	-	N/A	
CPUC Rule 2 Transparency (Notice)	Low	New SDG&E Customers are not being provided written notice regarding the accessing, collection, storage, use, and disclosure of Covered Information upon registering a new account. New customers receive a confirmation email upon registration which contains a link to the *Privacy Notice*. While this link is also a requirement under Rule 2b (and should be included on all electronic correspondence to customers), it does not replace the requirement to provide a written notice when confirming a new customer account. Customers that receive a paper monthly statement are provided the *Privacy Notice* as an insert in their first bill. Customers that have opted for paperless billing receive an email with a link to a site where all inserts for the month may be viewed.	Management should consider providing customers with SDG&E's *Privacy Notice* upon registering a new account. For paperless customers, this may be in the form of an email containing an attachment with SDG&E's *Privacy Notice* and for non-paperless customers, this could be an additional flier sent out after the customer registers a new account.	SDG&E's position is that the notice is sent in a reasonable amount of time based on the language of the standard. When a customer signs up for service with an email address, SDG&E emails the customer a link to the SDG&E privacy center that contains the Privacy Notice as well as other important privacy content including the company's website privacy policy, and the company's CCPA policy. Further, paperless customers receive an electronic copy of the Privacy Notice with their first eBill. For customers who prefer paper-based communication or do not provide an email address, SDG&E ensures the customer receives a written copy of the Privacy Notice in their first paper bill.
CPUC Rule 3 Purpose Specifications	Low	SDG&E's *Privacy Notice* provided to customers states that the customer may contact SDG&E if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.	Management should consider updating SDG&E's *Privacy Notice* to include the consequences customers may face if choosing to limit the collection, use, storage, or disclosure of their Covered Information.	SDG&E will add language to better clarify the consequences of limiting the collection, use, storage, or disclosure of Covered Information to its Privacy Notice.

CPUC Rule 4 Individual Participation (Access and Choice)	-	-	N/A	
CPUC Rule 5 Data Minimization	-	-	N/A	
CPUC Rule 6 Use and disclosure Limitations	Medium	Current SDG&E standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, KPMG observed inconsistent or missing privacy and security provisions in several sampled vendor contracts, which do not align to formal regulatory requirements.	Management should consider reviewing third-party contracts involving sharing Covered Information and ensure the contracts include the required standard language to enhance customer privacy protection and help ensure Covered Information is properly managed by third parties.	SDG&E's intention is always to include such language when Covered Information is involved. SDG&E reviews its supply management process to ensure that the appropriate language is included in contract templates that involve Covered Information. The specific language in SDG&E templates is sometimes subject to negotiations between SDG&E and vendors. However, in those circumstances where language is negotiated, SDG&E still requires in totality a level of protection consistent with the regulatory requirements.
CPUC Rule 7 Data Quality and Integrity	-	-	N/A	
CPUC Rule 8 Data Security	Medium	One SDG&E application storing Covered Information did not meet the baseline Sempra security requirements for user authentication and audit logging during the covered period.	Management should consider implementing the baseline Sempra Cybersecurity control requirements to adequately protect Covered Information stored and processed within the application.	SDG&E takes the security of systems that house Covered Information very seriously. When vulnerabilities are found in 3rd party hosted applications SDG&E works closely with the supplier to mitigate such vulnerabilities. The supplier mitigated the authentication vulnerability in Feb 2022 and is expected to mitigate the other shortly.
CPUC Rule 9 Accountability and Accounting	Low	SDG&E has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors	Management should consider implementing a process to automatically assign the required Covered Information training to contractors with access to Covered Information upon their on-boarding. This will help to ensure contractors are properly trained in a	SDG&E has requested an employee and contractor outreach and communication resource, which includes training, in its next GRC filing to address concerns with contractors receiving timely privacy training. Further, SDG&E is evaluating its process for capturing new contractors in favor of

		engaged after the training was initially launched.	timely manner on how to access, collect, store, use, and disclose Covered Information.	solutions that automate the inclusion of newly on-boarded contractors to the SDG&E privacy training content as soon as they are processed.
	Medium	SDG&E has a process in place to identify contractors with access to Covered Information and to assign relevant trainings regarding how to use, store, or process Covered Information. However, SDG&E is unable to enforce contractor trainings and therefore, completion rates could be lower than deemed reasonable.	Management should consider implementing a process to enforce contractor training completion. This could include follow-up emails, as well as escalation procedures (e.g., management involvement or termination of access to SDG&E systems) for contractors who have not completed the training in a timely manner.	SDG&E has requested an employee and contractor outreach and communication resource, which includes training, in its next GRC filing to address concerns with contractors taking the privacy training in a timely fashion. SDG&E is evaluating methods to enforce contractor training, including escalation procedures and termination of access to SDG&E systems.

Appendix I - Detailed assessment procedures and results

CPUC RULE 2 – Transparency (Notice)

Overall assessment result	**Exception noted:** New SDG&E Customers are not provided written notice regarding the accessing, collection, storage, use, and disclosure of Covered Information upon registering a new account. New customers receive a confirmation email upon registration, which contains a link to the *Privacy Notice*. While this link is also a requirement under Rule 2b (and should be included on all electronic correspondence to customers), it does not replace the requirement to provide a written notice when confirming a new customer account. Customers that receive a paper monthly statement are provided the *Privacy Notice* as an insert in their first bill. Customers that have opted for paperless billing receive an email with a link to a site where all inserts for the month may be viewed.

CPUC Rule 2	**Rule description**	
b		**When provided:** Covered entities shall provide written notice when confirming a new customer account and at least once a year shall inform customers how they may obtain a copy of the covered entity's notice regarding the accessing, collection, storage, use, and disclosure of Covered Information and shall provide a conspicuous link to the notice on the home page of their website, and shall include a link to their notice in all electronic correspondence to customers.

Assessment procedures	Assessment test results	Exceptions
1. Assess 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 SDG&E's *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Gas)* and noted it provides guidance to SDG&E employees regarding: — how to use and protect CEUD, — how the notice is provided to customers, and what it must include, — how customers can control their energy usage data, and — how SDG&E must only collect, store, use, or disclose only as much CEUD as necessary or authorized by the CPUC to meet specific operational or business needs. 1.b. Reviewed SDG&E's intranet site and noted SDG&E's formal privacy framework is based on the Generally Accepted Privacy Principles (GAPP), which helps organizations design and implement comprehensive privacy programs. 1.c. Viewed links to the *Privacy Notice* and *Privacy Policy* on SDG&E's website. SDG&E's *Privacy Notice* informs customers why SDG&E collects energy usage information, how long SDG&E retains energy usage information, when SDG&E shares energy usage information, how to view energy usage information online, and how to view the *Privacy Notice* online. 1.d. Visited SDG&E's website and noted the homepage contains a link to the privacy center where privacy-related links are attached, including: *Privacy Policy*, *Privacy Notice*, *California Consumer Privacy Act Policy*, *California Consumer Privacy Requests*, and *Protecting Customer Privacy*. 1.e. Met with SDG&E's Privacy Team and was informed there are three mechanisms used to share the *Privacy Notice*: — A billing insert sent to new customers with their first bill — A billing insert sent every year (around April) — SDG&E's website Customers enrolled in paper billing receive a paper copy of the *Privacy Notice*. Customers enrolled in paperless billing receive an email with a link to the webpage containing SDG&E billing inserts.	

Assessment procedures	Assessment test results	Exceptions
	1.f. Met with members of the Privacy Team and was informed the *Privacy Notice* is reviewed annually and no updates have been made since 2019. If changes to the *Privacy Notice* are made, customers are informed with a billing insert and the *Privacy Notice* on the website is updated.	
2. Assess whether a procedure exists to assess whether new customers receive written notice of the Company's privacy notice upon registration and annually thereafter.	2.a. Met with members of SDG&E's Privacy Team and was informed customers receive the Company's *Privacy Notice* as a billing insert with their initial bill and annually thereafter. The *Privacy Notice* is also publicly available on the SDG&E website. 2.b. Reviewed an example *Account Registration Confirmation* email sent to customers upon registration. This email contains the link to SDG&E's website privacy page, which includes a link to the *Privacy Notice*. The *Privacy Notice* contains a telephone number, email address, and postal address customers can use to request a hard copy of the *Notice*. Although a link is provided to the *Privacy Notice*, the customer is not provided a written copy (via email or mail) of the *Privacy Notice* upon registration. 2.c. Reviewed the *Privacy Notice Annual Bill Insert* and noted it contains a copy of the *Privacy Notice* and SDG&E's *Privacy Policy* web address. This insert also includes contact information to request a current or prior version of the *Privacy Policy* and obtain answers to any privacy questions, concerns, or complaints. 2.d. Reviewed the *Privacy Notice* and noted SDG&E updates the document as necessary and when required by the CPUC and would inform customers of the update through information provided with the bill or via SDG&E's website. 2.e. Reviewed the *Privacy Policy* and noted SDG&E reserves the right to add to, change, modify, or update the policy by posting a revised version on their website. Any revisions are effective immediately upon posting and date of modification is updated in the policy. 2.f. Emailed privacy@sdge.com on 10/25/2021 and asked for prior versions of the *Privacy Notice* in effect during the period between 2017 through 2020. Received an email response from SDG&E's Privacy Team on	New SDG&E Customers are not provided written notice regarding the accessing, collection, storage, use, and disclosure of covered information upon registering a new account. New customers receive a confirmation email upon registration which contains a link to the *Privacy Notice*. While this link is also a requirement under Rule 2b (and should be included on all electronic correspondence to customers), it does not replace the requirement to provide a written notice when confirming a new customer account. Customers that receive a paper

Assessment procedures	Assessment test results	Exceptions
	10/27/2021 containing copies of *Privacy Notices* effective 06/27/2017 and 10/21/2019.	monthly statement are provided the *Privacy Notice* as an insert in their first bill. Customers that have opted for paperless billing receive an email with a link to a site where all inserts for the month may be viewed.
3. Assess whether SDG&E provides notice to customers on an annual basis and when signing up new customers as required by the CPUC regulation.	3.a. See CPUC Rule 2b(2) for Test Results. 3.b. Visited the SDG&E website https://www.sdge.com/bill-inserts and noted billing inserts for each month from 2017 to 2021 can be viewed online, including the annual *Privacy Notice* insert.	See exception noted in Rule 2b(2).

CPUC Rule 2 c(1)-(2)	Rule description	**When provided:** 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.

Assessment procedures	Assessment test results	Exceptions
1. Review SDG&E'S methods for providing customers notice about their privacy and accessing the *Privacy Notice*.	1.a. See CPUC Rule 2b for Test Results. 1.b. Met with members of SDG&E's Privacy Team and was informed customers receive the Company's *Privacy Notice* with their first bill and annually thereafter. 1.c. Visited SDG&E's publicly available website and noted there is a link to "Privacy Center" is at the bottom of the homepage, which brings the user to privacy-related documents, including links to the *Privacy Policy* and *Privacy Notice*.	
2. Assess 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. Reviewed SDG&E's *Privacy Notice* and noted customers can provide feedback regarding the *Privacy Notice*. 2.b. Reviewed SDG&E's *Privacy Notice* and noted it includes normal font sizes, appropriate spacing, and does not seem longer than necessary to convey the requisite information.	
3. Assess whether SDG&E'S *Privacy Notice* is written in an easy-to-understand language.	3.a. Performed a Flesch-Kincaid reading level test on the *Privacy Notice* and noted that it was written at a college-level Flesch-Kincaid reading level (13th grade). 3.b. Performed a Flesch-Kincaid reading level test on the *Privacy Policy* and noted that it was written at a college-level Flesch-Kincaid reading level (15th grade). 3.c. Noted the *Privacy Notice* and *Privacy Policy* are available in 19 languages. They can be translated online through Google Translate directly on the website.	

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

Assessment procedures	Assessment test results	Exceptions
1. Understand the procedures in place to identify covered entities and assess whether the effective date is indicated in the relevant documentation.	1.a. Reviewed the *Privacy Notice* and noted it identifies SDG&E as the covered entity and states October 21, 2019 as the effective date. 1.b. Reviewed the SDG&E *Privacy Notice* available online and noted a section informing customers how to access past and current *Privacy Notices*. Customers may call 1-800-411-7343, mail their request to the address provided for the Customer Privacy P.O. Box, or email privacy@sdge.com. 1.c. Reviewed SDG&E's *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Gas),* and noted the document identifies a 'covered entity' as: — SDG&E or any third party that provides services to SDG&E under contract — Any third party who accesses, collects, stores, uses, or discloses covered information pursuant to an order of the Commission, unless specifically exempted, who obtains this information from an electrical or gas corporation — Any third party, when authorized by the customer, that accesses, collects, stores, uses, or discloses covered information relating to 11 or more customers who obtains this information from SDG&E	
2. Understand how the regulatory requirements, management review and approval process works, including potential alterations of the privacy policies.	2.a. Met with members of the Privacy Team and was informed SDG&E has not made any changes to the *Privacy Notice* since 2019. While there is no formally documented procedure, if a change was made, SDG&E's Privacy Team would send the proposed changes to the Legal Department for approval before implementation. Changes to the *Notice*	

Assessment procedures	Assessment test results	Exceptions
	are made if there are significant changes to the business or if the CPUC orders SDG&E to make a change. 2.b. Met with Regulatory Attorneys and was informed if the Commission were to adopt a new decision, the Regulatory Lawyers socialize this decision to necessary business groups. It is then the responsibility of the respective business unit to implement the decision.	
3. Inspect original and revision dates of policies to assess if actual updates/edits are made before approvals.	3.a. Met with members of SDG&E's Customer Privacy Team and was informed SDG&E last updated the *Privacy Notice* in 2019 due to an audit completed in 2017. This update was reviewed and approved by the Legal Department. The last revision to the SDG&E *Privacy Notice* and *Privacy Policy* was on October 21, 2019. 3.b. Met with members of the Privacy Team and observed an email communication via screenshare evidencing the review and approval of the *Privacy Notice* by the Privacy Program Manager for changes to the *Privacy Notice* from 2019. 3.c. Observed redline edits and comments from members of the Privacy Team on the most current *Privacy Notice* from 2019.	
4. Assess how SDG&E informs customers of any alterations to the Privacy Notice and where prior versions will be made available to customers.	4.a. Reviewed the *Privacy Notice* and noted it informs customers that changes to the *Notice* will be made as necessary and will be communicated through information provided with the customer's bill, as well as on SDG&E's website. The website provides customers with a telephone number, an email address, and a mailing address where individuals can request a current or prior version of the *Privacy Notice*.	
5. Observe whether SDG&E'S *Privacy Notice* identifies the title and contact information (including email address, postal address, and telephone number) of an official at SDG&E, who can assist the customer with potential privacy questions, concerns, or complaints.	5.a. Reviewed SDG&E's *Privacy Notice* and noted it includes contact information where customers can provide comments and concerns regarding the *Privacy Notice*. The contact information includes an email address (privacy@sdge.com), a mailing address directed to the Customer Privacy P.O. Box, and a phone number (1-800-411-7343).	

Assessment procedures	Assessment test results	Exceptions
6. Assess whether a specific person or group within SDG&E is responsible or accountable for privacy and security policy development, implementation, monitoring, enforcing, and updating.	6.a. Reviewed the SDG&E Privacy Intranet site and noted the OCP is the team responsible for helping SDG&E employees understand the Company's obligations to protect customer privacy. 6.b. Reviewed *SDG&E's Privacy Job Descriptions* for key OCP team members and noted: — Privacy Manager of the Customer Privacy Program oversees ongoing activities related to development, implementation, maintenance, and adherence to company policies and procedures covering the privacy of, and access to, customer information in compliance with federal and state laws and the company's privacy regulations. — Senior Privacy Standards Advisor leads the development, publication, and implementation of privacy standards and controls, project and process design reviews, privacy audits and Privacy Impact Assessments (PIA), privacy risk analyses, testing of privacy controls, and privacy trainings. — Customer Information Management (CIM) Advisor is responsible for CIM business processes and applications along with business processes and program goals related to customer information management and data sharing with third parties. — Privacy Project Specialist provides support to the SDG&E OCP. 6.c. Reviewed the *Compliance Management Framework Matrix* and noted SDG&E's OCP works with Regulatory Affairs and Legal department to stay informed of regulatory requirements. OCP collaborates with business units to socialize and comply with applicable rules and regulations. 6.d. Met with members of the Privacy Team and was informed the Privacy Steering Committee meets about once a month and includes the Legal Department, Vice Presidents, the Chief Information Officer, and Cybersecurity. The Privacy Steering Committee directs the Privacy Team. When the CPUC considers changes to legislation, the Privacy Team informs the Privacy Steering Committee and discusses potential impacts.	

CPUC RULE 3 – Purpose specification

Overall assessment result	**Exception noted:** SDG&E's *Privacy Notice* provided to customers states that the customer may contact SDG&E if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.

CPUC Rule 3	Rule description	**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.
a(1)-(3)		

Assessment procedures	Assessment test results	Exceptions
1. 1. Assess 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.a. Reviewed the *Privacy Notice* online and noted it provides: — The kinds of information that will be collected from and about customers — How that information will be collected, used, and protected — In what cases customer information will be disclosed to third parties and the type of companies (e.g. consulting organizations, engineering firms, and energy-efficiency providers) — To whom customer information will be potentially disclosed in the outlined circumstances (e.g. subpoena, emergency responders, as ordered by CPUC or as required by law) 1.b. Met with members of the Privacy Team and was informed SDG&E does not share Covered Information with third parties for Secondary Purposes. 1.c. Reviewed SDG&E's *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Gas)* and noted the document provides the definition of primary uses of Covered Information:	

Assessment procedures	Assessment test results	Exceptions
	— Provide or bill for electrical power or gas — Provide for system, grid, or operational needs — Provide services as required by state or federal law or as specifically authorized by an order of the Commission — Planning, implementing, or evaluating demand response, energy management, or energy efficiency programs under contract with an electrical or gas corporation, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission	
2. Assess whether SDG&E tracks the categories of agents, contractors and other third parties to which they disclose Covered Information for a primary purpose.	2.a. Reviewed SDG&E's *List of In-Scope Business Partners/Vendors* and noted the document lists vendors who have access to Covered Information. 2.b. Reviewed SDG&E's *2020 Annual Privacy Report* submitted to the CPUC and noted SDG&E disclosed Covered Information to 1,065 third parties during the 2020 calendar year, which included suppliers, contractors, vendors under contract with SDG&E, local governments, academic researchers, state and federal agencies who properly requested the data, and customer authorized third parties. 2.c. Was informed by SDG&E's Supply Management Team the ITVMO provides guidance regarding performance of systematic assessments and tracking of IT vendors, including those with Covered Information access. 2.d. Reviewed the *Privacy GreenLight Standard* and noted Privacy GreenLight is SDG&E's system for disclosing aggregated customer data as approved by the CPUC without customer consent. This system enables SDG&E to comply with CPUC privacy decisions, the CPUC Energy Data Access Decision, and CCPA. 2.e. Reviewed SDG&E's *Consumer Information Processing Standard* and noted Consent to Share (CtS) is the system used for managing and tracking consumer consent forms (*CISR* forms) to release data to third parties. Green Button is SDG&E's system for managing self-service customer authorizations.	

Assessment procedures	Assessment test results	Exceptions
	2.f. Met with Community Choice Aggregator Managers, Billing Analysts, a Senior Market Advisor, and a Senior Business Services Analyst, and was informed SDG&E contracts with Energy Service Providers (ESPs) and Community Choice Aggregators (CCAs), who have access to Covered Information and provide energy to SDG&E customers. Each third party must undergo an on-boarding process with SDG&E and enter into a Service Agreement. Once SDG&E and the third party have a signed service agreement, the third party must use the agreement to register with the CPUC. 2.g. Reviewed templates for *Service Agreements* with ESPs, CCAs, and an Non-Disclosure Agreement (NDA) for CCAs providing energy to SDG&E's Customers and have access to Covered Information. Noted these third parties must sign service agreements defining roles and responsibilities of both parties, including provisions with mandatory safeguards around customer information.	
3. Assess whether a procedure exists to assess whether new customers receive notice of SDG&E'S reasons for collecting, using, storing, or disclosing Covered Information.	3.a. See CPUC Rule 2b(1) Test Results.	
4. Assess whether SDG&E effectively monitors compliance with its collection, use, storage, and disclosure practices.	4.a. Reviewed the *SDG&E Consumer Information Stewardship Attestation Standard* and noted the OCP manages the process by which Data Stewards attest that they are in compliance with these requirements as long as they are processing SDG&E customer personal information (PI). Data Stewards (a director or senior manager responsible for processing one or more consumer PI data elements) are required annually to undergo the *Consumer Personal Information Attestation*, which asks a series of questions regarding their processing of SDG&E consumer PI, which includes their Covered Information. 4.b. Met with members of the Legal Team and was informed if any changes to CPUC regulations occur, the Legal Team communicates these new regulations to the business unit affected. The business unit is responsible for implementing changes.	

Assessment procedures	Assessment test results	Exceptions
	4.c. Reviewed documentation associated with Internal Audits conducted in 2021 and noted there were no audits conducted related specifically to Covered Information in 2021. Multiple audits were conducted related to cybersecurity controls and no issues were identified.	

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E'S *Privacy Notice* addresses the retention of Covered Information.	1.a. Reviewed the *Privacy Notice* and noted SDG&E keeps energy usage information only for as long as necessary to serve customers. The *Notice* also indicates retention periods vary based upon the specific circumstances and business needs but will most typically be 8-10 years.	

CPUC Rule 3	Rule description	Customer limitation:
c(1)		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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E'S *Privacy Notice* and processes address customers' ability to view, inquire, or dispute their Covered Information or other PII.	1.a. Reviewed the *Privacy Notice* and noted it identifies how customers may contact SDG&E with questions and to find out how they can limit, view, or dispute their disclosed information. Customers can contact SDG&E by calling 1-800-411-7343, emailing privacy@sdge.com, mailing the provided address to the Customer Privacy P.O. Box, or by signing into the customer's online account at https://myaccount.sdge.com/ to edit their profile. 1.b. Reviewed SDG&E's *Bill Insert* to customers, which includes SDG&E's *Privacy Notice* providing customers with the option to find out how they can limit, view, or dispute their disclosed information by contacting SDG&E at: — Telephone: 1-800-411-7343 — Email: privacy@sdge.com — U.S. Mail: SDG&E, Attn: Customer Privacy, P.O. Box 129831, San Diego, CA 92112-9831 1.c. Reviewed an example *Account Registration Confirmation* email. This email contains the link to SDG&E's online privacy page, which includes privacy-related links such as the *Privacy Notice*. This online version of the *Notice* contains a telephone number, email address, and postal address customers can use to request a hard copy of the *Privacy Notice*. 1.d. Met with members of the Customer Contact Center Operations Support team and was informed customer complaints are entered into the complaint tracking system by an Associate Supervisor. When a Contact Center Representative receives a complaint, the information is emailed to a supervisor, who then registers the information into the tracking system. Data privacy complaints are subsequently routed to the Complaint Resolution Team.	

Assessment procedures	Assessment test results	Exceptions
	1.e. Met with members of the Complaint Resolution Team and was informed the Privacy Team assists with privacy complaints the Complaint Resolution Team is unable to resolve. 1.f. Reviewed a customer complaint sent to SDG&E's OCP email (customerprivacysupport@sdge.com) and noted the customer received a timely response addressing their concerns. 1.g. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-411-7343) for inquiries regarding their bills and account management. The customer bill also states if the customer is not satisfied with SDG&E's response, the customer can contact the CPUC at 1-800-649-7570 or by visiting www.cpuc.ca.gov/complaints/.	

CPUC Rule 3	Rule description	Customer limitation:
c(2)		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E'S *Privacy Notice* addresses the explicit/implicit consent required to collect, use, and disclose Covered Information and other personal information.	1.a. Reviewed the *Privacy Notice* and noted it addresses implicit customer consent for primary purposes and explicit consent required for third party information sharing: — Sharing with third parties: SDG&E may share Energy Usage information with technology providers, consulting organizations, engineering firms, and energy-efficiency providers to better serve customers. — Other Third Parties: SDG&E may ask customers for permission to share Energy Usage information with other companies required to follow SDG&E's privacy policies. — Sharing at your choice: Customers can designate third parties to receive their information. — Sharing for other purposes: SDG&E may release Energy Usage information as required by warrant or subpoena, to emergency responders in the case of imminent threat to life or property, as required by the CPUC, or as required by law. The *Privacy Notice* also addresses customers rights to limit the information provided to SDG&E. See CPUC Rule 3c(2) Test Results. 1.b. Reviewed the *Customer Information Processing Standard* and noted several processes for customers to access their data or share data with third parties: — CtS: SDG&E's privacy control for managing consumer consent forms (*CISR* forms). — Green Button: SDG&E's system for managing self-service customer authorizations that meet certain criteria and allows customers to review energy usage data online.	

Assessment procedures	Assessment test results	Exceptions
	— Other consumer authorizations: SDG&E will honor specific written or verbal requests by consumers to disclose their personal information to a third party that do not meet CtS or Green Button standards. There are strict processes to validate customers and document their consent.	
2. Assess whether SDG&E communicates to individuals the consequences of denying consent.	2.a. Reviewed the *Privacy Notice* and noted customers can find out how to limit, view, or dispute their information by contacting SDG&E through mail, email, or by phone. However, no consequences are stated if the customer chooses to limit their Covered Information. 2.b. Reviewed SDG&E's Website *Privacy Policy* and noted it states the customer may choose not to provide any Personal Information and they will still be able to access most portions of the website. 2.c. Reviewed the *Smart Meter Opt-Out Program* publicly available at SDGE.com and noted for customers who do not wish to have advanced meters installed on their homes, they can opt-out by submitting an online form, submitting an opt-out request by visiting an SDG&E branch, or calling SDG&E at 1-877-357-8528. This web page also includes a FAQ section with details and additional costs associated with opting out.	The SDG&E *Privacy Notice* provided to customers states that the customer may contact SDG&E if they would like to "find out how you can limit, view, or dispute your disclosed information"; however, there are no stated consequences if the customer limits the collection, use, storage, or disclosure of their Covered Information.
3. Inspect SDG&E'S systems where Covered Information is collected to assess whether customers' implicit or explicit consent preferences are captured (before data transfer).	3.a. Reviewed SDG&E's website *Privacy Policy* and noted it states: "By using our website or obtaining any product or service through our website, 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 website." 3.b. Reviewed SDG&E's customer account online registration process and noted to create an account, the customer must check a box acknowledging review and agreement to SDG&E's *My Account Terms and Conditions*, which includes a checkbox to acknowledge and confirm agreement.	

Assessment procedures	Assessment test results	Exceptions
	3.c. Reviewed SDG&E's *Website Terms and Conditions* (publicly available at https://www.sdge.com/sdgecom-terms-and-conditions) and noted: — "Users must discontinue use of this Web site immediately if they do not agree or accept all these Terms and Conditions." — "Our privacy policy pertaining to any information obtained by Company from this Web site can be found in the Privacy section of the Web site. Additional privacy rules may apply as stated in portions of this Web site restricted for specific User services." 3.d. Reviewed *My Account Terms and Conditions* and noted by selecting the "I Agree" button when registering for a My Account portal, customers are confirming to comply with the *My Account Terms and Conditions*.	

CPUC RULE 4 Individual Participation (Access and Control)

Overall assessment result	No exceptions noted.

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E'S *Privacy Notice* addresses the provision of access to individuals to their Covered Information.	1.a. Reviewed SDG&E's *Privacy Notice* and noted that customers can view their usage data online accessing *'My Account'* at https://myaccount.sdge.com/ 1.b. Reviewed the *My Account* portal in the link above and noted it provides detailed instructions for customers to register and create an account to retrieve their energy usage data. 1.c. Reviewed SDG&E's *Welcome Email to New Customers* and noted it contains a link to *My Account* portal. The email also informs customers via *My Account* they can make payments, manage bills, and review energy usage information.	
2. Assess whether SDG&E'S internal policies describe the process for providing customers with access to their Covered Information.	2.a. Reviewed the *Customer Information Processing Standard* and noted it addresses how SDG&E provides customers with access to their Covered Information. This document is available to all employees in SDG&E's intranet and notes SDG&E will not disclose customer information without customer consent except for a primary purpose or specific exceptions. SDG&E has several platforms and systems to track customer authorizations and to disclose customer information: — CtS: SDG&E's system for managing consumer consent forms. — Green Button: SDG&E's system for managing self-service customer authorizations that meet certain criteria and allows customers to review energy usage data online. Green Button provides customers	

Assessment procedures	Assessment test results	Exceptions
	and authorized third-parties with access to up to 13 months of energy usage data. — Other approved consumer authorizations through the use of CISR forms. 2.b. Met with members of the Customer Contact Center and was informed a customer can call the Contact Center or go to a Service Branch to request Covered Information. Before any information is released, ESSs are required to authenticate the customer by obtaining the customer's full name, contact phone number, and last four digits of their SSN. If a customer does not have an SSN, they can be authenticated by their four-digit PIN.	
3. Assess whether customers can access their Covered Information in a detailed, yet easy-to-read format.	3.a. Inspected the *My Account* portal on the SDG&E website and noted SDG&E provides customers with access to Green Button, an energy management tool, to view their energy use, see their current bill and a forecasted bill for the month. Customers can review hourly, weekly, or monthly energy use, analyze bills to see fluctuations, and learn about energy-saving actions. 3.b. Obtained and inspected a screenshot of a customer's online My Account portal and noted customers can access their energy usage information on the main dashboard page. Customers have 24-hour access to their energy usage data. To download their *Energy Usage Report*, customers can log in using their unique credentials, select the option "Usage," then "Green Button Download," and finally click "Download". 3.c. Reviewed a sample *Energy Usage Report* downloaded from *My Account* and noted the document is an Excel file containing energy usage data in a detailed, easy-to-read format for a specified date range. 3.d. Reviewed a sample weekly email alert sent to customers signed up for weekly emails. This email provides customers with information such as billing cost to date, projected bill cost, electric and gas usage to date, and electric and gas use during on-peak, off-peak, and super off-peak hours. 3.e. Met with members of the Customer Contact Center and was informed customers may call to request or discuss their energy usage data.	

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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has a process in place for providing customers with access to grant and revoke authorization for secondary uses.	1.a. Reviewed the *Customer Information Processing Standard* and noted SDG&E will not disclose or share consumer information without customer consent except for a primary purpose or specific exceptions (including legal processes such as warrants or subpoenas, to emergency responders in the case of imminent threat to life or property, or as ordered by the CPUC). 1.b. Reviewed *Rule 34: Release of Customer Data to Third Parties* and noted SDG&E customers can grant and revoke a third party's access to their data by completing a CISR form or through the Green Button application. 1.c. Reviewed the Green Button page on SDG&E's public webpage and noted SDG&E uses Green Button to allow customers to access their energy use data. There is also a "Green Button Download My Data" option that allows customers to send their energy usage data to thirdparty applications of their choice. 1.d. Met with members of the Privacy Team and was informed that any disclosure of data for secondary use requires authorization via a completed *CISR* form in CtS or Green Button. 1.e. Inspected a sample *CISR* form and noted customers can provide authorization and consent for disclosure of specific account information to designated Third Parties for intervals such as single time consent, one year authorization, or customer timed interval (as designated by the customer and for a period of up to three years).	

Assessment procedures	Assessment test results	Exceptions
	1.f. Met with members of the Customer Operations Team and was informed CtS contains a "revoke" button that customers can press to revoke third party authorizations. 1.g. Reviewed a screenshot of the "revoke" button within CtS and noted customers can press this button to immediately revoke authorization (previously granted through a CISR form) to third parties with access to their data.	
2. Assess whether SDG&E has a process in place for customers to access their Covered Information and dispute its accuracy and completeness.	2.a. Reviewed SDG&E's *Privacy Notice* and noted customers can contact SDG&E through phone, web, or mail with questions, concerns, or complaints. 2.b. Obtained and inspected a screenshot of a customer's online account and noted customers can access their CEUD through a "Usage" link. The resulting report organizes the customer's gas and electric usage data by billing period. In addition, the online account provides customers with access to usage and other personal information, as well as the ability to dispute potential incorrect/inaccurate data. 2.c. Met with members of the Customer Contact Center and was informed that once a customer is validated, an ESS can use "impersonation mode" where they can view what the customer sees on their screen. This allows ESS's to better assist customers with any inquiries or concerns. There is also an "account assist" function where ESS's can complete different functions that update a customer's *My Account*. 2.d. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-411-7343) for inquiries regarding their bills and account management. The customer bill also states if the customer is not satisfied with SDG&E's response, the customer can contact the CPUC at 1-800-649-7570 or by visiting www.cpuc.ca.gov/complaints/.	
3. Assess whether SDG&E has a process in place to make corrections or amendments to the collection, storage, use, or distribution of Covered	3.a. Met with members of the Customer Contact Center and was informed that all ESS personnel can assist a customer with updating or correcting account information and resolve common inquiries or complaints. If the ESS is unable to resolve the inquiry or complaint, it will be escalated to the Customer Complaint Resolution Team.	

Assessment procedures	Assessment test results	Exceptions
Information upon a customer's request.	3.b. Met with members of the Complaint Resolution Team and was informed all complaints are logged into their complaint tracking system. Privacy related complaints are routed to the Customer Complaint Resolution Team. If the team is unable to resolve a privacy related complaint, it is routed to the Privacy Team for resolution. 3.c. Reviewed SDG&E's *Privacy Notice* and noted customers may contact SDG&E through phone, email or mail with any questions, concerns, or complaints. The document also includes contact information for how customers can "limit, view, or dispute their disclosed information." The contact information includes an email address (CustomerPrivacySupport@semprautilities.com), a mailing address directed to Customer Privacy and a phone number (1-800-411-7343). 3.d. Reviewed SDG&E's *SmartMeter Opt-Out* webpage, publicly available at www.sdge.com/residential/smart-meter-opt-out/smart-meter-opt-out-program, for customers who do not wish to have advanced meters installed for their homes. The website provides guidance to customers and necessary forms to complete as well as a phone number they can use to opt-out. 3.e. Reviewed a sample customer bill and noted it provides the customer a phone number (1-800-411-7343) to contact for inquiries regarding their bills and account management. The customer bill also states if the customer is not satisfied with SDG&E's response, the customer can contact the CPUC at 1-800-649-7570 or by visiting www.cpuc.ca.gov/complaints/.	

CPUC Rule 4	Rule description	Disclosure pursuant to legal process:
c(1)-(6)		(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 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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has procedures in place to help ensure proper handling and documentation of any Covered Information data disclosures for legal reasons.	1.a. Reviewed SDG&E's *Privacy Notice* and *Privacy Policy* and noted SDG&E does not release Covered Information without customers' written consent except under certain circumstances. These circumstances include disclosures: — pursuant to a legal process (such as a warrant or subpoena) — to emergency responders in the case of imminent threat to life or property — as ordered by the CPUC — as required by law 1.b. Reviewed SDG&E's *Customer Information Processing Standard* and noted SDG&E informs customers what types of personal information is collected and how it is used. Every employee is required to understand and comply with all company policies regarding customer privacy. SDG&E will not disclose or share consumer information without	

Assessment procedures	Assessment test results	Exceptions
	customer consent except for the case of specific exceptions or a primary purpose. 1.c. According to *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Gas)*, primary purposes are: — providing or billing for electrical power or gas, — providing for system, grid, or operational needs, — providing services as required by law or as authorized by the Commission, or — planning, implementing, or evaluating demand response, energy management, or energy efficiency programs. 1.d. Met with Managing Litigation Attorney and Senior Litigation Paralegal and was informed SDG&E has procedures in place for handling and documenting Covered Information data disclosures for legal purposes. Inquiries pursuant to legal process are handled by the Litigation Group (within the Law Department) that reviews them for authenticity and other legal requirements prior to disclosing the requested data. SDG&E only discloses customer data with customer consent, or if a lawful subpoena or warrant is present. 1.e. Met with Managing Litigation Attorney and Senior Litigation Paralegal and was informed SDG&E's Litigation Group is responsible for processing all subpoenas served to the company. SDG&E's process to respond to subpoenas is as follows: — Subpoenas are reviewed by the Litigation Group. If the subpoena is requesting Covered Information, then a *Notice of Disclosure of Energy Usage Data* letter is sent to the customer. The customer has seven days to contest the subpoena. If the customer does not respond, their information is not redacted. — All responsive documents are combined into one PDF and provided to the requesting party through the Sempra Electronic Data Transfer site. — All records are retained in the document management system.	

Assessment procedures	Assessment test results	Exceptions
	— Subpoenas are tracked in an ongoing log.	
2. Inspect documentation regarding disclosure of Covered Information pursuant to a legal purpose to test whether SDG&E properly handled the demand.	2.a. Reviewed a redacted version of the *Notice of Disclosure of Energy Usage Data* letter sent to specific customers listed in the subpoena prior to SDG&E disclosing Covered Information and noted customers are provided a seven (7) day notice to respond to the demand pursuant to SDG&E's legal process. The letter stated: "Pursuant to the provisions of the Decision, SDG&E is required to give you this notice and inform you that it will not produce the records until a date at least seven days from the date of this letter, thereby providing you time to appear in court and contest the subpoena should you choose to do so. Enclosed for your review is a copy of the subpoena."	
3. Inspect the Annual Report submitted to the Commission to test whether SDG&E reported the number of demands received for disclosure of customer data pursuant to a legal process and the number of customers whose records were disclosed.	3.a. While the 2021 Annual Privacy Report is not available as of the date of this report, KPMG had access to and reviewed SDG&E's *2020 Annual Privacy Report* submitted to the CPUC on April 30, 2021 and noted during 2020, SDG&E received 416 demands for disclosure pursuant to legal processes and 1,062 customers had records disclosed pursuant to those legal process.	

CPUC Rule 4 d	Rule description	**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).

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has procedures in place to help ensure proper handling and documentation of any Covered Information data disclosures in situations of imminent threat to life or property.	1.a. Reviewed SDG&E's *Privacy Notice* and noted SDG&E may disclose Covered Information without customer's prior consent to emergency responders in the case of imminent threat to life or property. 1.b. SDG&E's *Statement of Intent Procedures* regarding such requests notes when an emergency responder requests the names and/or telephone numbers listed on an account, this information may be released. If this situation occurs, the disclosure of the customer's information is documented on the account, and a supervisor should be notified immediately. 1.c. Met with Managing Litigation Attorney and Senior Litigation Paralegal and was informed they respond to all subpoenas served. A call for imminent threat would typically come through the Call Center. In this instance, Call Center employees are told to follow the *Statement of Intent Procedures*.	
2. Inspect documentation regarding disclosure of Covered Information in situations of imminent threat to life of property.	2.a. See CPUC Rule 4d(1) Test Results. 2.b. There were no demands received for disclosure of customer data pursuant to imminent threat to life or property during the covered period.	
3. Inspect the Annual Report submitted to the Commission to assess whether 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	3.a. While the 2021 Annual Privacy Report is not available as of the date of this report, KPMG had access to and reviewed SDG&E's *2020 Annual Privacy Report* submitted to the CPUC on April 30, 2021 and noted during 2020 SDG&E received zero (0) requests to disclose Covered Information pursuant to situations of imminent threat to life or property.	

Assessment procedures	Assessment test results	Exceptions
customers whose records were disclosed.		

CPUC RULE 5 Data Minimization

Overall assessment result	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.

Assessment procedures	Assessment test results	Exceptions
1. Assess 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 SDG&E's *Privacy Notice* and noted customer information is kept only for as long as necessary to serve them 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 8-10 years. 1.b. Reviewed the *Consumer Information Processing Standard* and noted only information required for a transaction or activity should be collected. Each department collecting consumer information is required to document how every data element collected will be used. 1.c. Reviewed *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and *Rule 33: Rules Regarding Privacy and Security For Energy Usage Data (Gas)* and noted SDG&E has the following data minimization practices in place: — Covered entities are to collect, store, use, and disclose only as much covered information as is reasonably necessary or as needed to accomplish a specific primary purpose. — Covered entities shall keep covered information for only as long as necessary or as authorized by the commission or the customer. — Covered entities shall not disclose to a third party more covered information than is necessary or as authorized by the Commission or the customer. 1.d. Met with members of the Privacy Team and was informed SDG&E does not collect any data not needed for a specific business purpose.	

Assessment procedures	Assessment test results	Exceptions
	1.e. Met with Billing Manager, Customer Operations Supervisor, and Collections Supervisor and was informed they follow a clean desk policy. While working from home, employees are required to still maintain the clean desk policy and cannot use personal printers or emails. 1.f. During a virtual walk-through of SDG&E's Escondido Branch Office, KPMG noted SDG&E has data minimization procedures in place, including shred badge access to the banking room and "view blocker" screen protectors on computers.	
2. Assess 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. Met with the Privacy Team and was informed that SDG&E does not disclose Covered Information for Secondary Purposes.	
3. Assess whether SDG&E has internal privacy policies addressing Data Minimization.	3.a. Reviewed the *Sempra Information Classification Guidelines* internal policy document and noted it outlines classification levels and protections required for information at each level. In addition, the standard states that generally, information should be limited to the fewest number of individuals to reduce the risk of compromise or misuse. 3.b. Reviewed SDG&E's *Consumer Information Processing Standard* and noted only information required for a transaction or activity should be collected. Each department collecting consumer information is required to document how every data element collected will be used. 3.c. Reviewed the *Sempra Code of Business Conduct* and noted employees are obligated to protect any confidential information they learn about or encounter in the workplace. The code states employees must protect personal employee, business partner and customer information, limiting access and usage only to authorized personnel and only for appropriate business purposes.	

Assessment procedures	Assessment test results	Exceptions
4. Assess whether SDG&E implements Data Minimization across User Access roles to systems and applications where Covered Information is stored, used, or processed.	4.a. During virtual walk-throughs of the SDG&E Customer Contact Center and Branch Office observed that employees practice Data Minimization principles and only access the information that is needed to complete the transaction or activity. 4.b. Reviewed the SDG&E *Consumer Information Processing Standard* and it was noted that only the information needed to complete a transaction or activity should be viewed or collected.	

CPUC Rule 5	Rule description	**Data retention:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E'S internal policies address a document retention policy covering all relevant aspects.	1.a. Reviewed SDG&E's internal *Information Management Policy* which applies to all Sempra employees and noted it includes the processes for preservation, organization, and disposal of all company related information. This policy also includes recordkeeping requirements designated to ensure records are appropriately classified, stored, and disposed of in accordance with business and applicable legal requirements. The policy includes links to the *Legal Hold and Preservation Policy*, *Information Security and Acceptable Use Policy*, *Information Management* site, and *Approved Information Repositories*, among others. 1.b. Reviewed SDG&E's *Records Retention Schedule* and noted the schedule provides detailed retention periods for all document classifications grouped by business functions, subjects, descriptions, and retention timeframes. 1.c. Reviewed SDG&E's *Wireless Communication Device Policy* and noted mobile devices are subject to the same retention periods set out in the *Information Management Policy*.	
2. Assess whether the SDG&E retention policies are periodically reviewed and updated where necessary.	2.a. Met with Regulatory Affiliate Compliance Manager and was informed that the record function (updating policies and record codes) is managed at Sempra. In addition, each SDG&E business unit is assigned an Information Coordinator. Records retention schedules for each business unit are reviewed by the assigned Information Coordinators at least annually. The Coordinators ensure their departmental record retention schedule remains accurate and updated. 2.b. Reviewed SDG&E's *Information Management Policy* and the *Records Retention Schedule* and noted both documents were updated during 2021.	

Assessment procedures	Assessment test results	Exceptions
3. Assess 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 Regulatory Affiliate Compliance Manager and was informed of the following: — Information Coordinators that are assigned to each business unit: i. ensure their departmental record retention schedule is updated and records are cleaned up ii. manage shared sites, ensure electronic sites are cleaned up, and manage reports received from electronic records services annually iii. are responsible for providing a status on records contained within reports received from electronic records services (for all records retained, a reason should be stated) iv. are required to take the *Records and Information Management Training* annually — An annual clean-up occurs from May to July where every department "cleans up" their records ensuring they are compliant with the *Records Retention Schedule*. Compliance certification for every department occurs annually from September to December. The certifications go through multiple level of approvals, concluding with approval from the Records Office. 3.b. Records can be disposed on-site through a third party or electronically. Records disposed are logged, however due to COVID-19, there was an exception for on-site disposal at closed locations during the covered period. These records will be disposed once offices reopen.	
4. Inspect evidence that SDG&E records are retained and disposed of in compliance with record retention policies.	4.a. Reviewed sample *Certificate of Destruction* as well as *Destruction Logs* for the covered period and noted they contain approvals for disposal. 4.b. Reviewed the *Information Management Certificate* required to be completed by a Senior Director, Director and/or Manager and noted the designated employee must sign and initial various items in a checklist to confirm that the department: — understands SDG&E's Information Management Policy, — complies with the Retention Schedule and approved storage locations, and	

Assessment procedures	Assessment test results	Exceptions
	— disposes of records when no longer needed or upon the disposal dates.	
5. Inspect evidence that SDG&E destroys documents that are no longer necessary or when the appropriate retention policy ends.	5.a. Reviewed multiple hard drive destruction logs and noted they contain approvals for disposal. 5.b. Observed locked shred bins at facilities containing Covered Information during a virtual walk-through of the SDG&E Customer Contact Center, Branch Office, Credit Operations, and Billing Operations Center. Noted a contracted third party performs on-site shredding of bin contents on a routine schedule. If additional shredding is needed, the facility employees request an additional pick-up from the third party.	

CPUC Rule 5	Rule description	Data disclosure:
c		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.

Assessment procedures	Assessment test results	Exceptions
1. Understand SDG&E'S privacy policies to assess 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.a. Reviewed internal SDG&E documentation and conducted interviews with SDG&E personnel and noted information can be shared with third parties via: — CtS: Customers must sign, approve, and upload a *CISR* form to CtS before SDG&E can disclose Covered Information with a third party — Green Button: Customers can download their energy reports from Green Button to share with third parties — Privacy GreenLight: SDG&E can share aggregated and anonymized data with approved third parties — Contractual signed agreements between SDG&E and approved vendors — As required by the CPUC — As required by legal processes 1.b. Reviewed the *Privacy Notice* and noted SDG&E describes practices related to sharing personal information with third parties and the reasons for information sharing. Specifically, SDG&E informs customers: — Primary Purposes: SDG&E may share Covered Information with vendors under contract with SDG&E, such as consulting organizations, engineering firms, or technology providers; — Customer's Choice: Customers can designate Third Parties to receive their Covered Information by providing written consent; — Other Purposes: SDG&E may release Covered Information pursuant to a legal process, to emergency responders in the case of imminent threat to life or property, or as ordered by the CPUC. 1.c. Reviewed the *Customer Information Processing Standard* and noted SDG&E employees are expected to ensure consumer information they	

Assessment procedures	Assessment test results	Exceptions
	interact with is accurate and compliant with applicable rules and tariffs. It is noted SDG&E would only disclose consumer information without customer consent for specific exceptions or a primary purpose. Consent-driven and non-consent-driven authorizations to disclose information are tracked within various SDG&E systems. 1.d. Reviewed the *Customer Information Processing Standard* and noted it outlines the three processes and systems SDG&E uses to share customer information: CtS, Green Button, and Privacy GreenLight. 1.e. Reviewed list of in-scope vendors identified as third parties with access to Covered Information during 2021 and confirmed there is a process to track third parties with access to Covered Information. Third parties are subject to contractual agreements, as well as to *Sempra's Supplier Code of Conduct*. 1.f. Reviewed the *Consent to Share Third Party Training Guide* and noted CtS is an online tool used to help customers manage their consent provided to share information with Third Parties. A *CISR* Form is required before SDG&E can share information with a requested third party. *CISR* forms enable SDG&E to track the type of information a Customer wishes to share with a Third Party and for how long. 1.g. Reviewed SDG&E's Privacy GreenLight Intranet site and noted Privacy GreenLight is the process followed for disclosing aggregate covered information as approved by the CPUC without customer consent. All third-party requests are to be entered into the program except emergency response requests, regulatory requests, subpoenas, and customer-initiated requests. 1.h. Reviewed CPUC-approved *CISR* form and noted customers must provide written authorization to SDG&E to allow a third party to receive customer information or act on the customer's behalf. In addition, the form states what rights are delegated to third parties, what information the third party is entitled to receive, and whether the authorization is provided on a one-time basis or on a longer-term basis (limiting duration to three years).	

Assessment procedures	Assessment test results	Exceptions
	1.i. Reviewed *Supplier Code of Business Conduct* and noted Sempra instructs third parties to keep non-public information confidential. All nonpublic information must be appropriately secured and protected. 1.j. Met with Customer Information Management Advisor and members of the Privacy Team and was informed SDG&E only shares Covered Information to third parties with prior customer written consent through the *CISR* process or authorization through Green Button. The customer must designate in the CPUC-approved *CISR* form the type of information shared and the specified time period for sharing the information. Only upon receiving the customer signed *CISR* form or authorization through Green Button will SDG&E disclose the requested information to the third party and for the designated purpose.	

CPUC RULE 6 Use And Disclosure Limitation

Overall assessment result	**Exceptions Noted:** Current SDG&E standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, KPMG observed inconsistent or missing privacy and security provisions in several sampled vendor contracts, which do not align to formal regulatory requirements.

CPUC Rule 6	Rule description	
c(1)-(3)		**Disclosures to third parties –** **(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 SDG&E disclosing the Covered Information shall, by contract, require the third party 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 SDG&E 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.

Assessment procedures	Assessment test results	Exceptions
1. Understand SDG&E' privacy policies to assess 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.a. Reviewed SDG&E's *2020 Annual Privacy Report* dated April 30, 2021 and noted SDG&E classified third parties with access to Covered Information into three categories: — Customer authorized third parties — Suppliers, contractors, and vendors under contract — Customer-authorized researchers or government requests 1.b. See CPUC Rule 5c for test results.	
2. Assess whether SDG&E informs customers that personal information is disclosed to third parties only for the purposes (a) identified in the Privacy Notice, and (b) for which the individual has provided implicit or explicit consent, or as specifically	2.a. Reviewed SDG&E's *Privacy Notice* and noted SDG&E only discloses customer information to: — Contracted third parties — Parties as ordered by the CPUC — Third parties with customer consent through CISR form — Legal processes via subpoena or warrant	

Assessment procedures	Assessment test results	Exceptions
allowed or required by law or regulation before data is disclosed to third parties.	— Emergency responders in cases of imminent threat to life or property 2.b. Reviewed *CISR Form 185-1000 Authorization to: Receive Customer Information or Act on a Customer's Behalf* and noted by completing the form, customers authorize a specified third party to request and receive the customer's data (such as billing records, account information, and usage data) stated on the form. Customers must specify whether this is a one-time authorization, one-year authorization, or determine an expiration date (limited in duration to three years). To complete the form, customers must provide their signature stating the customer understands that they may cancel this authorization at any time by submitting a written request. 2.c. Reviewed the *Green Button* page on SDG&E's public webpage and noted customers can choose to share up to 13 months of energy usage data with selected third parties by logging into the *My Account* portal.	
3. Assess 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. Reviewed Sempra's *Supplier Code of Business Conduct* and noted the document outlines policies regarding information protection and confidentiality: — Information may only be used for Sempra Energy business and must be in accordance with all applicable laws, regulations, and contractual obligations. — Nonpublic information could include, but is not limited to, customer, employee, or other business information and should be limited to only information required to perform the contracted work. — Nonpublic information must be kept confidential and only be disclosed to those subject to Sempra's confidentiality provisions if it is necessary for the performance of the Supplier's work. — Nonpublic information must be appropriately secured and protected. — Suppliers will not make any announcements or release any information on behalf of Sempra Energy without prior and appropriately authorized written consent of Sempra Energy. 3.b. Inspected confidentiality and non-disclosure clauses in a sample *Standard Services Agreement (SSA)* between SDG&E and a supplier with access to Covered Information and noted it includes a definition of	

Assessment procedures	Assessment test results	Exceptions
	Covered Information, governance regarding the handling of customer information, and the consequences of improper disclosure. 3.c. Inspected confidentiality and non-disclosure clauses in sample *Mutual NDA* between SDG&E and a supplier with access to Covered Information and noted it includes a definition of confidential information, governance regarding the handling of customer information, and consequences of noncompliance. 3.d. Reviewed *Sempra Procurement Policy* and noted it outlines policies, procedures, and guidance for procurement purposes, and noted contractors are not allowed to commence work until a valid contract is in place. 3.e. Met with members of SDG&E Customer Contact Center and was informed that customers must be authenticated using their account information (i.e., complete address, last four digits of social security number (SSN), account number, or four-digit PIN) before discussing any customer information. If a customer does not have an SSN, SDG&E can assist the customer creating a four-digit PIN for the customer to be authenticated with. 3.f. Reviewed templates for service agreements with ESPs, CCAs, and an NDA for CCAs providing energy to SDG&E customers and noted ESPs and CCAs must sign SSAs with SDG&E defining roles and responsibilities of both parties, including provisions with mandatory safeguards around customer information. 3.g. Met with Billing Analysts, CCA Billing Operations Manager, and CCA Strategy and Policy Manager, and was informed ESPs must be registered with the CPUC prior to executing a service agreement with SDG&E. 3.h. Obtained and inspected a sample SSA and NDA executed between SDG&E and a vendor with access to Covered Information and noted they include confidentiality and data privacy provisions mentioning potential breach of contract damages should the third party not adhere to contract terms. Additionally, the contracts restrict the use of confidential information solely for purposes stated in the contract.	

Assessment procedures	Assessment test results	Exceptions
4. Understand whether third-party contracting documentation is consistent with the SDG&E' policies and procedures.	4.a. Met with members of the Privacy Team, Portfolio Manager for Supply Management, and Value Capability Manager for the Cybersecurity Risk and Compliance Team (CEC) and was informed of the following: — Legal reviews all technology contracts with a dollar value of $2,000,000 or more. Contractors are not allowed to commence work until a valid contract is in place. — Once a contract is signed, the contracted business unit is responsible for managing and enforcing the contract. — Agreement templates include a confidentiality clause. In addition, technology contracts also include SDG&E's *Information Security Requirement* legal terms and conditions. — Three different risk assessments may occur before a contract is executed: i. IT VMO Risk Assessment: conducted on all vendors, regardless of type of data shared. ii. CEC Risk Assessment: a deeper risk assessment only assessing certain vendors with access to SDG&E systems containing sensitive information or vendors engaging in higher-risk activities, in which the *Information Security Third Party Assessment and Attestation* form is issued. iii. IS Risk Assessment: performed based on type of vendor and data shared. In this case SDG&E takes steps to further understand the criticality of data and relationship with vendor. 4.b. Reviewed *Sempra Procurement Policy* and noted Supply Management and the contract-issuing party are responsible for ensuring other interested parties (project managers, risk management, regulatory, tax, etc.) review issued contracts. The Law Department reviews and approves contracts with a dollar value of $2,000,000 or more and contracts involving high risk products or services. Contractors are not allowed to commence work until a valid contract is in place. 4.c. Was informed by the Privacy Team that before onboarding a vendor, basic information is gathered through the *Customer Privacy Third-Party Review Questionnaire* and entered in a database. IT VMO then conducts	

Assessment procedures	Assessment test results	Exceptions
	the IT VMO Risk Assessment in which they ask multiple vetting questions to decide whether further risk assessments, including comprehensive IS/cybersecurity assessments (i.e., IS or CEC Risk Assessments) and risk ratings, are needed. 4.d. Reviewed the *IS Third Party Assessment and Attestation* form, used in the CEC Consulting Risk Assessment, and noted contractors are asked a series of security infrastructure, monitoring, compliance, and data security questions before a contract is executed. 4.e. Reviewed *Sempra Procurement Policy* and noted contractors cannot commence work until a valid contract is in place. 4.f. Reviewed SDG&E S*upplier Code of Business Conduct* which states customer information should only be used for Sempra Energy business and all nonpublic information must be kept confidential. 4.g. Reviewed *Information Security Requirements*, included in technology agreements with SDG&E's third parties, and noted contractors verify their products contain necessary security measures to meet data protection regulations and laws. 4.h. Inspected contract template *Additional Terms and Conditions* included in SDG&E's standard contract template used when contracting with third parties and noted it includes a confidentiality clause governing the handling of Covered Information. Contractors shall not disclose any confidential information to other third parties, including SDG&E affiliates that produce energy or energy-related products or services, without prior written consent and approval from SDG&E or as required by law. The contract template also states a potential breach of contract damages if the third party does not adhere to contract terms.	
5. Inspect sample evidence of acknowledgments/certifications from third parties regarding compliance with SDG&E' data privacy policies.	5.a. Obtained and inspected a sample of five executed vendor contracts with access to Covered Information. It is noted that privacy and security provisions exist in contracts; however, language inconsistencies that do not align to formal regulatory requirements were identified in two of the contracts sampled. 5.b. Reviewed two sample *IS Third Party Assessment and Attestation* forms in which SDG&E asked vendors a series of security questions. Vendors	Current SDG&E standard contract templates contain privacy and security provisions aligned with CPUC requirements. However, KPMG observed inconsistent

Assessment procedures	Assessment test results	Exceptions
	provided responses related to their security requirements and signed to attest they provided truthful responses.	or missing privacy and security provisions in several sampled vendor contracts, which do not align to formal regulatory requirements.
6. Assess whether SDG&E has a process in place to review contract compliance for third parties accessing or receiving Covered Information.	6.a. Was informed by the Privacy Team that SDG&E's CEC Team completes the CEC Risk Assessment on a third party if they host or store company data. Depending on the risk score assigned to the third party, another assessment will occur every one, three, or five years. Reviews of third parties are triggered if: — a company will host or store data outside of the SDG&E network — SDG&E receives a breach notification of a company that hosts or stores SDG&E data — a vendor with access to Covered Information has a breach 6.b. Inspected contract template *Additional Terms and Conditions* included in SDG&E's standard contract template used when contracting with third parties and noted it includes a "Right to Audit" clause in which SDG&E has the right to conduct compliance reviews, audits, or other verifications on the contracted company. Noted this audit clause was not executed for vendors with access to Covered Information during the covered period. 6.c. Reviewed *IS Third Party Assessment and Attestation* form and noted SDG&E asks a series of security infrastructure, monitoring, compliance, and data security questions that contractor is required to fill out before a contract is executed.	

CPUC Rule 6	Rule description	Secondary purposes:
d(1)-(3)		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E engages in Secondary Purposes, and assess 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. Met with Customer Information Management Advisor and was informed SDG&E requires customer consent through a *CISR* form prior to disclosure any Covered Information to third parties. The customer must designate in CPUC-approved *CISR* form the type of information shared and the specified time period for sharing the information. 1.b. Reviewed *My Account Terms and Conditions* (https://www.sdge.com/my-account-terms-and-conditions) and noted if a customer wishes to disclose any information on their bill, including usage information, to another person or third party, the customer must provide SDG&E with a written signed authorization through a *CISR* form. 1.c. Met with the Privacy Team and was informed SDG&E does not share Covered Information for Secondary Purposes without customer consent.	
2. Assess whether SDG&E has secondary use authorization forms customers sign to	2.a. See CPUC Rule 6c(2b) test results.	

Assessment procedures	Assessment test results	Exceptions
authorize use of Covered Information for secondary uses.		
3. Inspect evidence that customer consent authorizing use of Covered Information for Secondary Purposes is documented.	3.a. Reviewed SDG&E's *CISR* form templates and noted by completing them customers can authorize a specified third party to request and receive specific customer data stated on the forms. 3.b. Met with SDG&E Customer Information Management Advisor and was informed when a *CISR* form is submitted to CtS, the system automatically reviews the form and completes multiple checks for accuracy. CtS compares customer account information from the billing and metering systems to customer account information on the form. If information does not match, an exception is triggered and requires an employee to manually review the form. Once approved, the form becomes active and data can be sent out.	

CPUC Rule 6	Rule description	Customer authorization:
e(1)-(3)		(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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether customers receive the Privacy Notice and must provide separate authorization if information is being used for a new Secondary Purpose.	1.a. See CPUC Rule 5c test results. 1.b. Reviewed the *CISR* form templates and noted customers can provide authorization and consent for disclosure of specific account information to designated third parties for intervals such as single-time consent, one year authorization, or for a specified period of time as designated by the customer (for a period of up to three years).	
2. Understand how customers are notified of their right to revoke any previously granted authorization and the process to do so.	2.a. Reviewed *Privacy Notice* and noted customers can limit or dispute third parties' use of previously authorized access to Covered Information. 2.b. Reviewed *CISR* Form *Authorization to Receive Customer Information or Act on a Customer's Behalf* and noted to complete the form, customers must provide explicit consent and sign an acknowledgment clause stating, "I understand that I may cancel this authorization at any time by submitting a written request." 2.c. Met with SDG&E Customer Information Management Advisor and was informed customers can revoke any previously granted authorization via the *CISR form*. Customers can revoke a form by logging into CtS and pressing the "revoke" button, sending an email to the privacy email stated in the *Privacy Notice*, or filling out the electronic revoke form. 2.d. Reviewed a screenshot of the "revoke" button within CtS and observed evidence this is an option offered to customers.	

Assessment procedures	Assessment test results	Exceptions
	2.e. Reviewed a sample *CISR* Form *Authorization to: Receive Customer Information or Act on a Customer's Behalf* and noted customers can specify what types of covered information is authorized as well as the duration of authorization. The specific types of information are included to be requested and/or received are: — Customer billing records, billing history and all meter usage data used for bill calculation — EPA Benchmarking — Copies of correspondence in connection with the customers' account — Investigations of the customers' utility bills — Special metering data in association with the account — Rate analysis — Rate changes — Verification of balances on customer accounts and discontinuance notices The specific duration of these requests are for: — Single-use authorization — One-year authorization — Custom authorization up to three years	

CPUC Rule 6	Rule description	Parity:
f		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has a process in place to allow customers to cancel authorization for any Secondary Purposes.	1.a. See CPUC Rule 6e(2) for test results.	

CPUC Rule 6	Rule description	**Availability of aggregated usage data:**
g		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 Covered Information because of the size of the group, rate classification, or nature of the information.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E' Privacy Notice or internal policies address the use of aggregate information.	1.a. Reviewed *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Gas)* and *Rule 33: Rules Regarding Privacy and Security for Energy Usage Data (Electric)* and noted SDG&E permits the use of aggregated usage data removed of all personally identifiable information. This data can be used for analysis, reporting, or program management only if the release does not disclose specific customer information. 1.b. Reviewed *Consumer Information Processing Standard* and noted customer information can be released to third parties for legitimate business reasons when it has been sufficiently aggregated, anonymized, or pseudonymized to hide customers' identity. 1.c. Reviewed *Customer Services Policy* and noted SDG&E follows CPUC Data Aggregation Standards noted in Decision 14-05-016. 1.d. Reviewed SDG&E's *Customer Privacy Guidelines* and noted this document addresses the use of aggregated information and defines aggregated and anonymized data: — Aggregated data is data that has no identifiable information to disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information. — Anonymized data is customer data from which all identifying information has been removed such that the customer cannot be identified or reasonably re-identified.	
2. Assess whether SDG&E has a procedure in place to help ensure aggregate information does not disclose or reveal specific Covered Information.	2.a. Met with members of the Privacy Team and was informed data aggregation rules are reviewed and monitored by the Privacy Team. 2.b. Reviewed SDG&E's Privacy GreenLight Intranet site and noted Privacy GreenLight is the process followed for disclosing aggregated covered information as approved by the CPUC without customer consent. All third party requests are to be entered into GreenLight except emergency	

Assessment procedures	Assessment test results	Exceptions
	response requests, regulatory requests, subpoenas, and customer-initiated. 2.c. Reviewed SDG&E *Privacy GreenLight Standard* and noted the GreenLight process includes the following steps: — A third party submits a request — The third-party request sponsor validates the third party — The data custodian verifies the request can be fulfilled — A third-party review is conducted by Legal, Cybersecurity, and Supply Management — The data request is approved by the Business Director, Privacy Director, and Chief Consumer Privacy Officer (approval levels depend on risk level) Once the third party no longer needs the data, the third party submits a certificate of destruction attesting they have followed proper disposal policies.	

CPUC RULE 7 Data Quality and Integrity

Overall assessment result	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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E' privacy policies address the quality of Covered Information and other Customer PII.	1.a. Reviewed *Sempra Employee Code of Conduct* and noted it includes policy is for employees to protect customer security and integrity of their information. 1.b. Reviewed SDG&E's *Supplier Code of Conduct* and noted third parties are required to maintain accurate records and disclosures. 1.c. Reviewed SDG&E *Information Protection Standard* and noted Information Owners of each business unit is normally a manager or director responsible for protecting Information Assets. 1.d. Reviewed *Consumer Information Processing Standard* and noted employees and contractors are to ensure they collect, store, use, and disclose accurate consumer personal information. 1.e. Reviewed SDG&E's *My Account Terms and Conditions* and noted it is customer's responsibility to ensure information in their *My Account* profile is current and accurate. Customers are instructed to update incorrect information promptly through their *My Account* portal or by contacting SDG&E's Customer Service by email or at 1-800-411-SDGE.	
2. Inspect sample communication to customers to assess whether SDG&E policies include customer data integrity.	2.a. Reviewed SDG&E *Privacy Notice* and noted customers can limit, view, or dispute their disclosed information by contacting SDG&E at: — Telephone: 1-800-411-7343 — Email: privacy@sdge.com — Mailing address to the Customer Privacy P.O Box 2.b. Reviewed SDG&E's *Website Terms and Conditions* and noted the User Account section places responsibility for preserving the confidentiality of	

Assessment procedures	Assessment test results	Exceptions
	log-on and user account information on SDG&E customers. The website *Terms and Conditions* also prompts customers to contact SDG&E with any questions or comments. 2.c. Reviewed screenshots of the *My Account* portal setup process and noted before customers can create an account, they must check a box acknowledging they agree to SDG&E's *My Account Terms and Conditions*, which states that customers have read and agreed to comply with the *My Account Terms and Conditions* addressing it is the customers' responsibility to provide accurate and up-to-date information.	
3. Assess 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. Reviewed SDG&E's *Consumer Information Processing Standard* and noted only information required for an activity or transaction should be collected. After use, customer information should be disposed of accordingly. Employees and contractors are to ensure the consumer personal information they collect, store, use, and disclose is reasonably accurate. 3.b. Reviewed the *Sempra Information Management Policy* and noted employees must read and certify they have read the policy and dispose of information accordingly. 3.c. Reviewed SDG&E's *Protecting Customer Privacy Procedures* provided to ESS's and noted there are procedures in place to comply with before providing information to customers. If a customer listed on the account wants to discuss their account, ESSs verify the caller's name and service address or just the account number. In addition, the last four digits of the customer's SSN or four-digit PIN is required. 3.d. Reviewed SDG&E *Privacy Notice* and noted retention of energy usage data and personal information is addressed: "SDG&E will keep your Energy Usage information only for as long as necessary to serve you and handle matters like billing disputes, inquiries and system planning. Retention periods vary based on the specific circumstances and business needs, but will most typically be for eight to ten years."	
4. Inspect sample evidence to assess whether procedures are in place to safeguard personal	4.a. Met with Customer Billing Manager and Customer Operations Analytics Supervisor and was informed bills that meet certain qualifications will trigger an exception (e.g., bills within various dollar thresholds, billing	

Assessment procedures	Assessment test results	Exceptions
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.	changes, unusually high bills, etc.). Exceptions are worked by a billing team member who reviews in detail a number of aspects of the customer's account to resolve the exception, including field orders, service orders, and meter data collection among others. A quality assurance process is also in place to manually review around 10-20 accounts a month. 4.b. Inspected SDG&E's *My Account* registration process and noted customers must agree to provide accurate and up-to-date information. 4.c. See CPUC Rule 7(3) for test results.	

CPUC RULE 8 Data Security

Overall assessment result	**Exceptions Noted:** One SDG&E application storing Covered Information did not meet the baseline Sempra security requirements for user authentication and audit logging during the covered period.

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

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has documented policies addressing security provisions for Covered Information: — Risk assessment and treatment — Security policy — Organization of information Security — Asset management — Human resources security — Physical and environmental security — Communications and operations management — Access control — Information systems acquisition, development, and maintenance — Information security incident management — Business continuity management — Compliance	1.a. Risk Assessment and Treatment – Reviewed the *Cybersecurity Engineering & Consulting - Risk Rating Procedure* and noted that there is a detailed security risk assessment methodology with the objective of determining the level of risk presented to the organization. This is accomplished through an interview process between the CEC Team, the project team, and key business stakeholders. This document also explains the procedure and remediation plans based on each Common Vulnerability Scoring System scoring model score. This policy is applicable and accessible to all employees of Sempra Energy and is published on the Sempra IS intranet site. 1.b. Risk Assessment and Treatment – Reviewed the *Risk Management Guide* and noted that Sempra has a comprehensive risk assessment guide with complete instructions for completing risk assessments, developing a risk response strategy, and monitoring and reporting risk status. Metrics are formally documented and aligned to ISO 31000 principles and guidelines. It was also noted that the risk assessment process is conducted on an annual basis. This policy is applicable and accessible to all employees of Sempra Energy and is published on the Sempra IS intranet site. 1.c. Security Policy – — Reviewed the *Cybersecurity Awareness Standard*, *Physical Security Policy,* and the *Corporate Security Standards*, and noted that these policies outline access controls to company facilities, conditions for entry, access control practices, badge access authorization, and	

Assessment procedures	Assessment test results	Exceptions
	security planning and equipment. These policies are published on the Sempra IS intranet site accessible to all Sempra employees, vendors, and contractors. — Reviewed the *Sempra Information Security SharePoint site* and noted that company's *Cybersecurity Policy & Procedures page* is accessible to all Sempra Employees, vendors and contractors and includes various cybersecurity policies, standards, guidelines, and procedures. 1.d. Organization of IS – Sempra Energy's IS is structured as a shared service for SDG&E, SoCalGas, and other non-regulated companies. Leadership starts from the C-Suite and flows down throughout the organization. There are cyber councils comprised of senior leadership that meet monthly to raise awareness and discuss current threat landscape. The IS function is broken down into four main categories 1) Governance Risk & Compliance (GRC), 2) Monitoring & Response (Operations Side), 3) Architecture & Engineering, 4) Program Management (Project and equipment, Capital Expenditure). The program is aligned to the National Institute of Standards and Technology Cybersecurity Framework. 1.e. Asset Management – Reviewed the *Hardware Asset Management Process* and the *Data Destruction & Media Sanitation Guidelines* and noted that these policies describe in detail the process for tracking the lifecycle of hardware IT throughout the assets lifecycle. These policies describe in detail the process by which Sempra employees and all affiliates shall handle data storage locations, retentions periods, data classifications, and the methods of destruction for each type of classified data classified, including Covered Information. These policies are applicable and accessible to all employees of Sempra Energy and are published on the Sempra IS intranet site. 1.f. Human Resources Security – Reviewed the *Employment Verification and Reference Checks Policy & Employment Eligibility & Hiring of Relatives Policy* and noted that there are requirements for preemployment background checks and reference checks and preemployment screening. These policies are applicable and accessible to all employees of Sempra Energy and is published on the Sempra IS intranet site. 1.g. Physical and Environmental Security – Reviewed the *Physical Security Policy & Corporate Security Standard* documents and noted that physical and environmental security requirements are formally documented.	

Assessment procedures	Assessment test results	Exceptions
	1.h. Communication and Operations Management – — Reviewed the *Encryption Standard* and noted that encryption requirements and remote access encryption requirements are formally documented. — Reviewed the *Email Management Standard* and noted that requirements for managing email communications are formally documented. — Reviewed the *Social Media Guidelines* and noted that expectations around Sempra personnel conduct while engaging in social media activity that relates in any way to Sempra Energy are formally documented. 1.i. Access Control – Reviewed the *Electronic Access Management Standard* and the *Identity & Access Management (IAM) Cybersecurity Standard* and noted that access control requirements are formally documented. 1.j. Information Systems Acquisition, Development, and Maintenance – Reviewed the *IT Portfolio Management Office (IT PMO) SharePoint site* and noted that the information systems acquisition, development, and maintenance process are formally documented. 1.k. IS Incident Management – Reviewed the *Cybersecurity incident Response Standard* and noted that cybersecurity incident management procedures are formally documented. 1.l. Business Continuity Management – Reviewed the *Information Technology Disaster Recovery Policy*, as well as the *Business Continuity Policy* and noted that business continuity management and IT disaster recovery requirements are formally documented. 1.m. Compliance – Reviewed the *Supplier Code of Business Conduct*, the *Information Security Policy,* and the *Information Protection Standard* and noted that the requirements for compliance with applicable privacy legislation and regulations are formally documented.	
2. Assess whether SDG&E' privacy policies and procedures cover protection of electronic and print media containing Covered Information from unauthorized	2.a. Reviewed the *Privacy Policy* and *Information Security Policy* and noted that these policies address how SDG&E employees, contractors and third parties should handle Covered Information. 2.b. Reviewed the *Data Destruction and Media Sanitation Policy* and noted that these policies describe in detail the process by which Sempra employees and all affiliates shall handle data storage locations, retentions	

Assessment procedures	Assessment test results	Exceptions
access, destruction, use modification or disclosure.	periods, data classifications, and the method of destruction of Covered Information.	
3. Assess 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. Reviewed the *Information Management Policy* and noted that "all directors (and managers reporting to VPs) and above shall certify annually that their department is in compliance with this policy." 3.b. Reviewed the *Code of Business Conduct* and noted "employees are required to complete compliance training and to acknowledge that they understand and will comply with the Code. Failure to adhere to the standards of conduct outlined in the Code could result in disciplinary action, up to and including employment termination." 3.c. Reviewed the *Risk Exception SharePoint Site* as well as the *Exception Form Sample* and noted that a formal exception is required to be submitted by risk owners who request exceptions from Sempra policies, procedures, standards, or requirements and must include a business justification and mitigation steps. Risk exceptions will expire after one year of the exception approval and require an annual extension if the requirement cannot be met.	
4. Review evidence of SDG&E providing customers with the Privacy Notice on the security mechanisms used by SDG&E to protect their Covered Information.	4.a. See CPUC Rule 2b for test results. 4.b. Reviewed the SDG&E *Privacy Notice* and noted that it addresses SDG&E's approach to securing the Covered Information provided by customers. 4.c. Reviewed the *Privacy Policy* and noted that "Sempra and its Sempra Companies respect the privacy of every employee and customer and collects and retains private, personal information only as required by law or for the company to operate effectively. We must protect and limit access to personal employee, business partner and customer information, limiting access and usage only to authorized personnel and only for appropriate business purposes."	
5. Review evidence that SDG&E' policies on Data Security are communicated to internal employees and contractors who have access to Covered Information.	5.a. Reviewed the *Information Security Policy* and the *Privacy Policy* and noted that these policies are published on the Sempra IS intranet site, which is accessible to all Sempra employees and contractors with network access, and it provides guidance on data privacy for Sempra Energy. 5.b. Reviewed the *Confidentiality Policy* and noted it is published on the Legal intranet site accessible to all Sempra employees and noted that "Sempra	

Assessment procedures	Assessment test results	Exceptions
	and the Sempra Companies respect the privacy of every customer. Sempra and the Sempra Companies collect and retains a certain amount of customer-specific information that is required to effectively provide reliable, safe, and cost-effective services for our customers. Sempra and the Sempra Companies have implemented policies and procedures that protect and limit access to customer-specific information and comply with all applicable laws that govern confidential customer information". 5.c. Reviewed the *Cybersecurity Awareness Standard* and noted that the company provides the employees and contractors with ongoing cybersecurity education and training. The program includes Cyber Champions, who are volunteers trained to foster strong relationships and communicate cybersecurity best practices throughout the organization.	
6. Assess 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. See CPUC Rule 8a (1d) for test results. 6.b. Met with Cybersecurity Risk & Compliance Manager and was informed that a CEC team has been established. The team provides regular updates on identified risks (e.g., cyberattacks, data loss) and the mitigation efforts. 6.c. Reviewed *the Cybersecurity Engineering & Consulting - Risk Rating Procedure* and noted that the team maintains risk management process for making management decisions on security, privacy, and risks. Formal approvals from Cybersecurity and Privacy teams are required prior to new production releases and upgrades. If a project does not meet the necessary cybersecurity control requirements, then a risk exception is documented and sent for review and approvals. 6.d. Reviewed the *Risk Management Handbook* and noted that it provides guidance to Sempra on how to implement the risk management framework. It was also noted that an annual risk assessment is required and along with regular vulnerability assessment scans on all systems storing Covered Information. 6.e. Reviewed the *System Monitoring Standard* and noted that Sempra has established and maintains a compliance monitoring and audit program.	
7. Review SDG&E' relevant policies to assess if SDG&E incorporates security into their SDLC.	7.a. Reviewed the *Release and Environment Management Standard* and noted that all software development must comply with secure coding principles and practices throughout stages gates across the SDLC. The	

Assessment procedures	Assessment test results	Exceptions
	requirements include secure coding, development and testing practices, security architecture design, and vulnerability management. 7.b. Met with Cybersecurity Risk & Compliance Manager as well as others from application/web development teams and was informed that Sempra uses an agile DevSecOps methodology, where security is moved forward within SDLC to ensure security is incorporated into the process. Product owners and scrum masters will obtain the necessary approvals from the Cybersecurity and Privacy teams throughout the process. 7.c. Reviewed the *Information Security Engineering & Consulting Process* and noted that it applies to all types of IT products including software development and technology infrastructure. There are eight (8) phases, from concept to implementing into production, and each phase details the purpose and IS supporting activities. The process also includes roles and responsibilities.	
8. Assess 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. Review of supporting documents *Physical Security & Corporate Security Policy* and noted that the physical access controls are in place to protect Covered Information. 8.b. Reviewed the *Sempra Information Security intranet site* and noted the following controls are in place to protect Covered Information. — Access is controlled by badge access readers — Visitor sign-in and escort procedure — Visitor/Parking forms to notify security visitor is coming into building 8.c. Reviewed the *Sempra Information Security intranet site* and noted the following controls are in place to protect Covered Information. — Access management — On-site guard services — Security training — Risk and intelligence analysis 8.d. Met with Corporate Security Manager and was informed that physical access controls are in place to protect Covered Information. Performed virtual site walk-throughs of Sempra Production Data Center, SDG&E Customer Contact Center, and SDG&E Billing Center and observed that the following controls are in place:	

Assessment procedures	Assessment test results	Exceptions
	— Security guards are on-site 24/7 — Access is controlled by badge access readers — Visitor sign-in and escort is required — Clean desk/Clear screen policy — Covered Information is stored in locked in cabinets — Office printers require secure print functionality to complete print job — Shredders and locked shred bins are located in the facilities	
9. Assess whether SDG&E has implemented procedures for protecting Covered Information including controls for physically securing all media.	9.a. Reviewed *Information Protection Standard* and noted that portable storage devices must be secured in a locked room, drawer, cabinet, or safe when not in use or unattended. 9.b. Reviewed the *Information Security Manager & User Standard* and noted that user requirements are outlined for actions that must be taken by any user to protect information and technology assets, including physically securing and encrypting media.	
10. Inspect whether physical records containing Covered Information are stored in locked cabinets or rooms restricting unauthorized access.	10.a. Performed virtual walk-throughs of key facilities such as SDG&E Customer Contact Centers, Branch Offices, and the Sempra Production Data Center and observed that badge access readers are installed throughout the facilities that may limit access to a particular area containing Covered Information. There are secure bins located throughout the facilities for securely discarding any sensitive information therein.	
11. Inquire of SDG&E' personnel to gain an understanding of the logical control procedures in place to prevent unauthorized access to Covered Information.	11.a. Met with IAM Manager and was informed that a privileged access management solution has been implemented which also provides password management and privileged session recording. The solution has been expanding to encompass more applications and business units. Further, additional logical controls have been implemented, including: — Access requests must be approved by system and information owners — Access accounts are provisioned based on a principle of least privilege — User access accounts are reviewed on a periodic basis	
12. Inspect evidence that logical controls are in place to prevent	12.a. Reviewed the *Electronic Access Management Standard & Service Account & Intelligent Automation ID Guidelines* and noted that formal	

Assessment procedures	Assessment test results	Exceptions
unauthorized access to Covered Information including user access provisioning and deprovisioning.	procedures are in place to help ensure authorized access and prevent unauthorized access. 12.b. Reviewed one (1) sample user access requests and one (1) sample access removal for a system storing Covered Information and noted that an email chain is used to process the requests. Reviewed screenshots of the user profiles before and after the access requests and access removals and noted that the users were provisioned and deprovisioned in accordance with documented policies and procedures. 12.c. Inspected system profiles for SDG&E in-scope systems storing Covered Information and confirmed that logical access controls are implemented on the systems in alignment with Sempra policy requirements.	
13. Review SDG&E' relevant policies to assess if physical controls are in place protecting Covered Information.	13.a. Reviewed the *Physical Security Policy* and noted that controls around the physical protection of Covered Information are documented, including responsibility for managing access to facilities and performing continuous monitoring of facility perimeter controls. 13.b. Reviewed the *Enterprise Records and Information Management (ERIM) Standard* and noted that the operations group within ERIM is responsible for managing physical records storage, including records with Covered Information. This includes maintaining a chain of custody and taking appropriate security and fire-retardant measures. 13.c. Performed virtual site walk-throughs of SDG&E Customer Contact Center, SDG&E Branch Office, and the Sempra Production Data Center that store Covered Information and observed that the physical access controls implemented were in alignment with Sempra policy requirements. 13.d. Validated through a virtual site walk-through of the Sempra Bill Print facility that the print operators could not see the Covered Information during the bill print and mail insert processes.	
14. Inquire of SDG&E' personnel to gain an understanding of the controls protecting physical access to systems storing Covered Information.	14.a. Met with Data Center Facility Manager, and was informed that the following physical security controls are in place: — Access to the facility is restricted, the front entry gate is equipped with access readers and motion detectors. The main front entrance door has an access reader and a mantrap. Cameras are placed throughout the facility and monitored by an on-site manned guard station.	

Assessment procedures	Assessment test results	Exceptions
	— Access to server rooms is restricted by a dedicated fence surrounding the area and maintained by an access management system. — Employees not assigned to the facility, contractors, and visitors are required to sign a visitor sheet and are escorted throughout the facility.	
15. Inspect evidence that physical access to sites and systems storing Covered Information is monitored and restricted.	15.a. See CPUC Rule 8a (14) for test results.	
16. Review SDG&E' relevant policies to assess if environmental controls are in place.	16.a. Reviewed the *Sempra Energy Utilities Critical Facilities Standards* and noted the following environmental controls implemented: — HVAC with chilled water to keep the temperature at an appropriate level — Condensers — Fire detection system, alarms, and fire suppression using a Halon and Sapphire system and sprinklers — Backup power supply and generators — Emergency power off, and leak detection	
17. Inquire of SDG&E' 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. Reviewed the *IT Disaster Recovery Policy* and noted that each tier includes recovery time objectives, recovery point objectives, impact descriptions, and recovery services. The policy also outlines roles and responsibilities. 17.b. Met with Data Center Facilities Manager and was informed that the appropriate environmental controls in place at the Production Data Center. 17.c. Performed a walk-through of the Sempra Production Data Center and observed the environmental controls implemented are in alignment with Sempra policy requirements.	
18. Assess whether SDG&E has the ability to transfer data to third parties using secure channels.	18.a. Met with OCP Manager and was informed that a third-party risk review process is required to be completed as part of new vendor approvals, including a PIA and an IS risk assessment if they have access to any customer or employee information.	

Assessment procedures	Assessment test results	Exceptions
	18.b. Met with Cybersecurity Risk & Compliance Manager and was informed that that there are multiple secure file transfers methods used by Sempra, and between Sempra and its third parties. 18.c. Inspected system profiles for systems storing Covered Information and noted that the various systems are configured to provide/support protocols for secured authentication methods.	
19. Assess whether 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. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that Sempra uses an Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). The IPS/IDS is deployed at multiple points on the network via the next-generation firewalls. Logs are sent to Security Information and Event Management (SIEM) tool and all alerts are monitored and reviewed by a 24/7 SOC. 19.b. Met with Cybersecurity Operations Manager, and was informed that there are controls in place to monitor attempts to exfiltrate data across the network boundaries: — A data loss prevention (DLP) tool is implemented to detect data leakage and exfiltration attempts of Covered Information across the network boundaries. — Once flagged, a DLP Analyst will review the incident and determine if it is a true positive. If a true positive is found, the incident is escalated to the appropriate departments. Any follow-up actions that may be needed are determined by Cybersecurity team. 19.c. Observed that the DLP tool is configured to flag instances of unauthorized data exfiltration across the network. 19.d. Reviewed the *Mobile Device Management Standard* as well as the *End User Computing Device Policy* and noted that mobile device management tool is implemented to manage mobile data leakage.	
20. Assess whether 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	20.a. See CPUC Rule 8a (19) for test results.	

Assessment procedures	Assessment test results	Exceptions
transfers while alerting information security personnel.		
21. Assess whether SDG&E has controls in place so that users cannot disable and modify security products or services.	21.a. Reviewed the *Information Security Manager & User Standard* and noted that there are policies in place prohibiting users from circumventing or disabling any technology asset security controls or configurations and from preventing automated updates or scans. 21.b. Met with Cybersecurity Operations Manager and was informed that the DLP agent and antivirus agents are installed on every workstation, and a daily health check is reported on the agent's health. It was noted that users do not have administrative access to disable or modify agents on workstations. 21.c. Inspected system profiles for systems storing Covered Information and noted that the various systems are configured with audit logging capabilities to detect system activity. In addition, audit logs are sent to the Sempra SIEM tool for centralized monitoring.	One SDG&E application storing Covered Information did not meet the baseline Sempra security requirements for user authentication and audit logging during the covered period.
22. Assess whether SDG&E officials understand the current threat landscape and potential threats to the organization by leveraging multiple threat feeds.	22.a. Met with Threat Vulnerability Management Manager and the Cybersecurity Risk & Compliance Director and was informed that there is a dedicated cyber threat Intelligence team that provides daily and weekly briefs to stakeholders documenting major events and threat hunting activities. Threat intelligence feeds are digested from a variety of sources including law enforcement, industry sources, and industry sharing forums. Threat sources are aggregated and correlated using enterprise security tools and reports are generated for various needs. In addition, analysts monitor the system continuously and address all items based on priority and triage and escalate the incidents based on information available to them, using detailed playbooks.	
23. Assess whether SDG&E scans source code for bugs and vulnerabilities before moving it into production.	23.a. Reviewed the *Information Security Engineering & Consulting Process* and noted that as part of the Information Technology Product Lifecycle security testing and assessments are performed to resolve risks and prepare for moving to production. Supporting artifacts, including scan results, source code, technical analysis is documented and reviewed prior to deployment into production. The Cybersecurity team works with vendors to remediate or mitigate all vulnerabilities.	

Assessment procedures	Assessment test results	Exceptions
24. Assess whether SDG&E' development/test environments are separate from the production environment, with access control in place to enforce the separation.	24.a. Met with Cybersecurity, Risk & Compliance Domain Architect and was informed that development, test, and QA environments are separated from the production environment using firewalls and access controls. 24.b. Inspected systems profiles for systems storing Covered Information and noted that they have separate environments for development, testing, production and/or quality assurance purposes. 24.c. Reviewed the draft *Nonproduction Environment Standard* and noted that production data should not be used in non-production environments, only testing and dummy data can be used in non-production environment. In addition, no customer PII, Internal, Confidential or Restricted data can be used in nonproduction environment.	
25. Assess 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.a. See CPUC Rule 8a (24) for test results. 25.b. Reviewed the *Release and Environment Management Standard* as well as the *Information Protection Standard* and noted that there are protection standards in place based on information classification that must be adhered to, regardless of the location of that information in the network. Covered Information requires the highest level of protection when stored, accessed, disclosed, transported, or disposed.	
26. Assess whether SDG&E utilizes a data masking tool to limit access to and protect Covered Information and other PII.	26.a. Performed virtual walk-throughs of the SDG&E Customer Contact Center and SDG&E Branch Office and was informed that PII is masked, and minimal information is obtained by customer service representatives to perform tasks. For example, once an SSN has been entered into the system, only the last four characters will remain visible to the agent, while the rest will be hashed out.	
27. Assess whether SDG&E' web applications use encryption when transmitting sensitive data across the network.	27.a. Reviewed the *Encryption Standard* and noted that information classified as confidential or restricted must be encrypted at all times (using the documented minimum encryption strength and protocols), while internal information must be encrypted when transported outside of the company. 27.b. Reviewed the *Information Protection Standard* and noted that "all confidential and restricted information must be encrypted at rest and while in transit when moving internally and externally outside SDG&E's network.	

Assessment procedures	Assessment test results	Exceptions
	27.c. Inspected systems profiles for systems storing Covered Information and noted that encryption-in-transit protocols are in place to safeguard Covered Information.	
28. Assess whether SDG&E has implemented an Intrusion Detection system within the environment to detect and generate log messages detailing events.	28.a. Reviewed the *Network Security Standard* and noted that network based IPS sensors are deployed inline on the dematerialized zone (DMZ) and secure zone network connection points that can prevent, capture, inspect network traffic for unusual attack mechanisms and detect compromise of systems through the use of signatures, network behavior analysis and other mechanisms to analyze traffic. 28.b. Met with Cybersecurity, Risk & Compliance Domain Architect and confirmed that SDG&E uses an IPS and IDS. The IPS/IDS is deployed at multiple points on the network via the next-generation firewalls at both the network perimeter as well as at several points internally. The generated logs SIEM tool.	
29. Assess whether SDG&E has implemented an Intrusion Prevention system within the environment to detect events and reject packets.	29.a. See CPUC Rule 8a (28) for test results.	
30. Assess whether SDG&E allows only limited access to network resource to vendors and third parties.	30.a. Reviewed the *Electronic Access Management Standard* and noted that contractors and vendors can be issued accounts for a defined period of time. In addition, the standard states that the principle of least privilege must always be used when establishing accounts. 30.b. Met with Supply Management Manager and Cybersecurity & Risk Manager and was informed that all third-party vendors are required to complete security risk assessments before onboarding any new vendors.	
31. Assess whether SDG&E has a formal process for approving and assessing all network connections and changes to the firewall and router configurations.	31.a. Met with Cybersecurity, Risk & Compliance Domain Architect, and was informed that Sempra has a formal process in place for approving connections and changes to Firewall and Router configurations. 31.b. Reviewed the *Sempra Change Management SharePoint page* and noted that all changes and clearances to Sempra IT production environments and systems must have an approved change request. The goal of the Sempra IT Change Management Process is to ensure proper planning, impact assessment, risk assessment, testing, coordination, and approval	

Assessment procedures	Assessment test results	Exceptions
	in order to minimize the risk to production and business processes associated with implemented changes.	
32. Assess whether SDG&E' firewall performs stateful inspection (dynamic packet filtering) to restrict network access.	32.a. Reviewed the *Firewall Standard* and noted that that Sempra employs firewalls that are capable of stateful protocol analysis and provide intrusion detection or prevention technology. 32.b. Met with Cybersecurity, Risk & Compliance Domain Architect, and was informed that Sempra uses next-generation firewalls that apply stateful protocol (dynamic packet filtering) to block unauthorized network traffic.	
33. Assess whether 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. Reviewed the *Firewall & Network Security Standard* and *Smart Meter Master Network Diagram* and noted that the use of an DMZ is required to manage communications between Sempra networks and untrusted networks and the Internet to limit inbound traffic.	

CPUC Rule 8	Rule description	**Notification of breach:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess 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 SDG&E's *Personal Information Breach and Notification Response Plan* and noted procedures to follow if an information breach occurs, including response team roles, process documentation, investigation into breaches, remediation, notifications sent, and program updates. Specific procedures are also mentioned if an information breach were to occur within a third-party vendor. In certain cases, an information breach within a third-party vendor could lead to contract termination. 1.b. Met with Chief Counsel for Technology and Business Services and was informed he receives a series of monthly reports containing any unauthorized disclosures (including Covered Information) from the Cybersecurity Group. 1.c. Met with Strategy and Operations Manager for Digital Enablement Services and was informed vendors are expected to self-report breaches. 1.d. Met with Portfolio Manager for Supply Management and Value Capability Manager for Cybersecurity Risk and Compliance and was informed if a breach were to occur, SDG&E's Cybersecurity Team would investigate the incident to find out what occurred, understand the risk, and ask the vendor to provide an explanation. 1.e. Met with Value Capability Manager of Cybersecurity Risk and Compliance and was informed if a third-party breach occurred, SDG&E would immediately disable vendor's access to the SDG&E online environment. After a breach investigation is completed, SDG&E's Investigation Team meets with security teams involved and discusses the investigation and how to improve processes to avoid further occurrences. SDG&E is constantly updating or creating "playbooks" for incident management as new situations arise.	

Assessment procedures	Assessment test results	Exceptions
2. Assess whether SDG&E' management has adequately reviewed the incident review process in place.	2.a. Met with Value Capability Manager of Cybersecurity Risk and Compliance and was informed the *Personal Information Breach and Notification Response Plan* is reviewed annually and updated as necessary. 2.b. Met with Value Capability Manager of Cybersecurity Risk and Compliance and was informed after a breach investigation is completed, SDG&E's Investigation Team completes an investigation review and updates the processes and procedures accordingly.	
3. Assess whether SDG&E can perform forensic analysis in the instance of a Covered Information data incident.	3.a. Met with Cybersecurity Operations Manager and was informed that forensics analysis is conducted in-house and can be performed in the event of an incident involving customer PII or Covered Information. Further, there is a contract in place with a third party in case forensic assistance is needed.	
4. Inspect sample evidence of breach incidents for the last 12 months.	4.a. Met with Value Capability Manager of Cybersecurity Risk and Compliance and observed via shared screen, a sample low-level unauthorized disclosure of Covered Information breach incident.	

CPUC Rule 8	Rule description	**Annual report of breaches:**
c		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E tracks the reporting requirement and assigns responsibility and accountability to the appropriate departments.	1.a. Reviewed SDG&E's *Procedure for Setting Up SDG&E Annual Privacy Report* and noted processes for the creation, approval, and submission of the *Annual Privacy Report* to the CPUC. SDG&E's Privacy Report Review Team (Privacy Director, Sempra Privacy Attorney, SDG&E Privacy Attorney, and the Regulatory Attorney) grants approval before the Regulatory Department submits final version to the CPUC. 1.b. Met with Chief Counsel for Technology and Business Services and was informed he receives a series of monthly reports containing any unauthorized disclosures (including Covered Information) from the Cybersecurity Group. He identifies and tracks the unauthorized disclosures to be included in the *Annual Privacy Report*.	
2. Assess whether SDG&E filed its Annual Report to the CPUC as required by the Privacy Decision.	2.a. Reviewed SDG&E's *2020 Annual Privacy Report* and noted it was submitted to the CPUC on April 30, 2021. The report identified one breach within the 2020 calendar year.	

CPUC RULE 9 Accountability and Auditing

Overall assessment result	**Exceptions Noted:** 1) SDG&E has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched. 2) SDG&E has a process in place to identify contractors with access to Covered Information and to assign relevant trainings regarding how to use, store, or process Covered Information. However, SDG&E is unable to enforce contractor trainings and therefore, completion rates could be lower than deemed reasonable.

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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E has a process in place to provide the Commission with the *Annual Privacy Report* or any other requested documentation	1.a. SDG&E made available for this assessment the following documents, in line with these CPUC requirements: — *Privacy Notice* and *Privacy Policy* provided to customers and made available to the public through SDG&E's website — Internal privacy and data security policies	

Assessment procedures	Assessment test results	Exceptions
	— Listing of agents, contractors, and third parties with access to Covered Information — Templates of secondary-use authorization form (*CISR* form) by which SDG&E secures customer authorization for Covered Information — Procedures for processes related to accessing, collecting, using, and disclosing Covered Information 1.b. Reviewed *Procedure for Setting Up SDG&E Annual Privacy Report* and noted the Privacy Team collects metrics from various business units through email communications to compile SDG&E's *Annual Privacy Report* content. Once compiled, the draft report is created and circulated to SDG&E's Privacy Committee for review. The reviewed draft report is then presented to SDG&E Regulatory Department for final revision and submission to the CPUC. 1.c. Met with Senior Counsel of Regulatory Law and two Regulatory Case Managers and was informed the process for compiling the *Annual Privacy Report* begins around February/March. A member of the Privacy Team compiles the report by gathering required information from all necessary business units. Multiple levels of review occur, including by the Privacy Team, Regulatory Team, multiple business units, and Legal.	

CPUC Rule 9	Rule description	**Customer complaints:**
b		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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E provides notice to its customers on how the customers can contact the Company for inquiries, complaints or disputes related to their personal information.	1.a. Reviewed SDG&E's *Privacy Notice* and noted customers can limit, view, or dispute their disclosed information by contacting SDG&E via email, through mail to the Customer Privacy PO Box, or by phone. 1.b. Reviewed the SDG&E website and observed SDG&E provides two phone numbers, an email address, and an online chat option under the "Contact Us" section. 1.c. Observed the *Annual Privacy Notice Bill Insert* and noted SDG&E provides existing customers a bill insert encouraging customers to review the *Privacy Notice* on an annual basis.	
2. Assess 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 SDG&E's *Customer Compliments, Comments, and Complaints* document and noted customer compliments, comments, and complaints are entered into a tracking system by a supervisor and then routed to the appropriate team. If the customer would like a call back in regards to their compliment, comment, or complaint, then it would be noted on the ticket in the tracking system. 2.b. Met with Customer Contact Center Operations Strategy Manager and a member of the Complaints Team and was informed all complaints, compliments, and comments are logged into a tracking system as a new ticket attached to a customer account by a supervisor. Ticket information includes the subject, service category (customer privacy is an option), incident category, type (including categories such as "complaint- CPUC," "complaint- presidential," and "complaint- general."), customer name, source, and description. Tickets are assigned to an "agent" within the Complaints Resolution Team to resolve the complaint. Noted outstanding complaints are tracked within the tracking system to be resolved in a timely manner.	
3. Assess whether SDG&E has a process to escalate disputes,	3.a. Met with Customer Comments, Compliments, and Complaints Operations Strategy Manager and a member of the Complaints Team and	

Assessment procedures	Assessment test results	Exceptions
complaints, and inquiries to help ensure resolution within a timely manner.	was informed the Customer Complaint Resolution Team resolves most escalated complaints SDG&E receives. If the Complaint Resolution Team is unable to resolve a privacy complaint, they escalate the complaint to the Privacy Team for assistance. 3.b. Met with Customer Comments, Compliments, and Complaints Operations Strategy Manager and a member of the Complaints Team and was informed for complaints received through the CPUC site, SDG&E has 20 days to provide a response to the customer.	
4. Inspect evidence that SDG&E tracks and resolves customer complaints consistent with SDG&E' policies.	4.a. Inspected a sample customer complaint, which was routed to the Privacy Team and noted the item followed the documented procedure for documenting, classifying, and resolving customer complaints. 4.b. Performed a walk-through via screen share of a complaint being entered into their complaint tracking system. The tracking system interface has a dashboard that tracks outstanding tickets. The dashboard also has an option to view all outstanding complaints which can be filtered to view privacy related complaints. 4.c. Performed a walk-through via screen share of how complaints are tracked, monitored and also those downloaded from the CPUC site and logged into their tracking system.	

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

Assessment procedures	Assessment test results	Exceptions
1. Review SDG&E' documented privacy awareness program materials to identify personnel who handle and access Covered Information.	1.a. Met with members of the Privacy Team and was informed all SDG&E employees are required to complete a training that includes sections regarding Covered Information. In addition, each business unit is assigned a "Privacy Pro" required to complete an additional training with supplementary privacy content. 1.b. Met with members of the Privacy Team and learned the *Supplemental Consumer Privacy Training* is required annually for all individuals that have access to Covered Information. The process to identify personnel required to take the supplemental training is detailed below: — To assign the training to SDG&E employees, SDG&E's Privacy Team looks at access control lists for systems that contain Covered Information and assigns the training to employees with access to these systems. All SDG&E employee trainings are assigned and tracked within the Learning Management System (LMS). — To assign the training to contractors, SDG&E's Privacy Team pulls a listing of contractors with access to systems containing Covered Information. The Privacy Team also reaches out to the managers of these contractors to ensure the contractors have access to and handle Covered Information. Contractors included in the resulting population are assigned the training. All contractor trainings are assigned and tracked within the Contractor Training System. The process to assign contractors the *Supplemental Consumer Privacy Training* occurs once a year. 1.c. Reviewed the *Learning Assignment Tool* and noted the procedures followed to assign trainings to SDG&E employees. 1.d. Reviewed the *Contractor Training System Assignment Guide* and noted within the Contractor Training System, contractors can be assigned to take the *Supplemental Consumer Privacy Training*. This guide also contains screenshots of the initial assignment email, first reminder	SDG&E has an annual process in place to assign contractors with access to Covered Information a supplemental Customer Privacy training. However, this training is not consistently rolled out to contractors engaged after the training was initially launched.

Assessment procedures	Assessment test results	Exceptions
	notification email, second reminder notification email, final reminder notification email, past due notification email, and completion notification email sent to contractors.	
2. Understand the awareness material and communications to SDG&E personnel to test how internal privacy policies are communicated to associates.	2.a. Met with members of the Privacy Team and was informed internal privacy policies were communicated to SDG&E employees and contractors through the following trainings: — All SDG&E employees are required to complete the *Cybersecurity Training* with a *Privacy Module* annually assigned through the LMS. New hires are required to complete these trainings upon onboarding. — SDG&E employees and contractors with access to Covered Information are required to complete the *Supplemental Consumer Privacy Training* annually. 2.b. Reviewed additional privacy awareness documents, including Privacy Points emails sent to Privacy Pros. The Privacy Pros socialize these communications to their respective business units. Some topics of reviewed Privacy Points include: SDG&E aggregation standards, Privacy GreenLight, passwords, and safely handling customer data. 2.c. Reviewed a *New-Hire Training Email* and noted privacy trainings must be completed before being granted access to necessary internal platforms. 2.d. Reviewed SDG&E's privacy intranet website containing links to internal privacy resources, trainings, actions to take to report security incidents, and other resources for company employees. 2.e. Reviewed SDG&E's *Customer Care Center Work@Home Program Agreement* and noted ESSs were required to sign this agreement before working from home due to COVID-19. Noted this agreement mentions that all company policies are still applicable.	
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	3.a. Reviewed enterprise-wide *Cybersecurity Training* with a *Privacy Module* and noted every employee is required to complete this training. The training consists of a video and quiz at the end. This training provides examples of customer information (including PII and Covered Information) and provides guidelines for the collection, storing, sharing,	

Assessment procedures	Assessment test results	Exceptions
these privacy and security training requirements.	and disposal of customer data. Employees must pass the quiz at the end to receive completion credit. 3.b. Reviewed the *Supplemental Consumer Privacy Training* script and noted this 15-minute video is assigned to employees and contractors that have access to Covered Information. Employees and contractors are required to complete and a 9-question quiz once the video has ended. This video discusses: — Privacy terms — Notice and consent — Data collection and minimization — Storage and protection of Covered Information — Use, retention, and disposal of Covered Information — Privacy data incidents 3.c. Met with members of the Privacy Team and was informed the Cybersecurity Team tracks completion of the *Cybersecurity Training* and the *Privacy Module* in the LMS. Once tracking logs are pulled, the Privacy Team manually reaches out to managers and directors of employees who have not completed the training. 3.d. Inspected the *Cybersecurity Training Tracker* for employees and noted at the end of 2021, 97.40% of SDG&E employees had completed the training. 3.e. Inspected *Supplemental Consumer Privacy Training Tracker* for SDG&E employees at the end of 2021 and noted 97.22% of employees with an "active" status had completed the training.	
4. Inspect evidence that contractors have completed privacy and security training requirements (e.g., training logs, certifications of compliance, etc.).	4.a. Met with members of the Privacy Team and was informed contractors are under contractual obligation to follow SDG&E data privacy rules; however, there is no formal process in place to enforce contractors to complete the training. 4.b. Inspected *Supplemental Consumer Privacy Training Tracker* for contractors and noted at the end of 2021, about 50% of contractors had completed the training.	SDG&E has a process in place to identify contractors with access to Covered Information and to assign relevant trainings regarding

Assessment procedures	Assessment test results	Exceptions
		how to use, store, or process Covered Information. However, SDG&E is unable to enforce contractor trainings and therefore, completion rates could be lower than deemed reasonable. As a result, contractors with access to Covered Information could be on-boarded and off-boarded and never complete the training.
5. Understand the privacy training required of third parties accessing Covered Information in order to test whether or not they are adequately equipped to handle Covered Information.	5.a. See CPUC Rule 9c (3b) for test results. 5.b. Met with members of the Privacy Team and was informed vendor contracts have explicit and thorough language to ensure third parties abide by corporate rules regarding data privacy and security. Third parties are contractually obligated to follow all SDG&E privacy rules. 5.c. Reviewed Sempra's *Supplier Code of Conduct* provided to contractors and noted policies regarding information protection and confidentiality: — Nonpublic information contained in electronic or physical form must be appropriately secured and protected. — Nonpublic information accessed by suppliers must be limited to only that information that is required to perform the contracted work. — If suppliers are granted access through electronic or physical means to Sempra Energy's nonpublic information to perform Sempra Energy-related work, the information may only be used for Sempra Energy business.	

Assessment procedures	Assessment test results	Exceptions
	— Suppliers must keep nonpublic information confidential and may only disclose nonpublic information if it is necessary for the performance of their work. Such disclosures may be made only to those people who are also subject to Sempra Energy's confidentiality provisions and have a legitimate business need to know. 5.d. Inspected a sample NDA and a sample SSA between SDG&E and a supplier with access to Covered Information and noted both contracts included confidentiality and non-disclosure containing a definition of confidential information, governance regarding the handling of customer information, and consequences for noncompliance. 5.e. Reviewed service agreement templates and sample executed contracts between SDG&E and ESPs, CCAs, and CTAs and noted the contracts require nondisclosure of confidential information (including confidential customer information) without SDG&E's consent unless any governmental, judicial, or regulatory authority is requiring such confidential information pursuant to any applicable law, regulation, ruling, or order. 5.f. Inspected a sample of executed vendor contracts and noted they include confidentiality clauses protecting SDG&E's confidential information. The contracts also state that contractor may be required to complete training at SDG&E's sole discretion.	

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 noncompliances 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.

Assessment procedures	Assessment test results	Exceptions
1. Assess whether SDG&E tracks the reporting requirements and assigns responsibility and accountability to the appropriate departments.	1.a. See CPUC Rule 9a (1) for test results. 1.b. Met with members of the Privacy Team and was informed the Privacy Team leads the filing of the *Annual Privacy Report*. They start compiling the report around December by reviewing any Cybersecurity disclosure incidents, inquiring with business units to find out who Covered Information is shared with, and meet with the Regulatory Council. They also review Privacy GreenLight to see what third parties received Covered Information. Once the information is compiled and the report is formulated, it is reviewed by Directors, Legal, and other business units before it is submitted to the CPUC. 1.c. Reviewed the *Procedure for Setting Up SDG&E's Annual Privacy Report* and noted the process for creation, approval, and submission of the *Annual Privacy Report* to the CPUC. SDG&E's Privacy Report Review Team (Privacy Director, Sempra Privacy Attorney, SDG&E Privacy Attorney, and the Regulatory Attorney) approve the report before the Regulatory Department submits the final draft to the CPUC.	
2. Assess whether SDG&E filed its Annual Report to the CPUC as required by the Privacy Decision.	2.a. Reviewed SDG&E's *2020 Annual Privacy Report* and noted it was submitted to the CPUC on April 30, 2021 and included: — The number of authorized third parties accessing Covered Information — The number of noncompliances with CPUC privacy rules or with contractual provisions required by the Privacy Rules known to SDG&E — The number of customers affected by each noncompliance and a description of each noncompliance	

Appendix II - Abbreviations used in this report

Abbreviation	Full name
CCA	Community Choice Aggregator
CCPA	California Consumer Privacy Act
CEC	Cybersecurity Engineering Risk and Consulting
CEUD	Customer Energy Usage Data
CIM	Customer Information Management
CISR	Customer Information Service Request
CPUC	California Public Utilities Commission
CtS	Consent to Share
DLP	Data Loss Prevention
DMZ	Demilitarized Zone

Abbreviation	Full name
ERIM	Enterprise Records and Information Management
ESP	Energy Service Provider
ESS	Energy Service Specialist
GAPP	Generally Accepted Privacy Principles
GRC	Governance Risk & Compliance
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
IS	Information Security
ISO	International Organization for Standardization
IT	Information Technology
IT PMO	Information Technology Portfolio Management Office
IT VMO	Information Technology Vendor Management Office
LMS	Learning Management System
LOB	Line of Business
NDA	Non-Disclosure Agreement

Abbreviation	Full name
OCP	Office of Customer Privacy
PI	Personal Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SDG&E	San Diego Gas and Electric Company
SDLC	Software/System Development Life Cycle
SIEM	Security Information and Event Management
SSN	Social Security Number
SSA	Standard Service Agreement

Appendix III - Stakeholders interviewed

#	Title	Organizational Unit	Date
1	Customer Privacy Project Manager	Customer Operations	11/12/2021
2	Customer Information Management Advisor	Customer Operations	11/12/2021
3	Senior Privacy Standards Advisor	Customer Operations	11/12/2021
4	Customer Information Management Analyst	Customer Operations	11/12/2021
5	Customer Information Management Advisor	Customer Operations	11/12/2021
6	QA & Analytics Manager - Audit Services	Audit Services	11/12/2021
7	Prin IT Auditor	Audit Services	11/12/2021
8	Audit Services Manager	Audit Services	11/12/2021
9	Value Capability Manager	Cybersecurity Risk & Compliance	11/15/2021
10	Print Domain Engineer - Cyber	Cybersecurity Risk & Compliance	11/15/2021

#	Title	Organizational Unit	Date
11	Strategy & Operations Manager	Digital Enablement Services	11/17/2021
12	Director - Cybersecurity, Risk & Compliance	Cybersecurity Risk & Compliance	11/17/2021
13	Customer Care Center Operations Support Supervisor	Customer Care	11/23/2021
14	Group Product Manager	Digital & SDGE Customer	11/29/2021
15	Product Owner Team Lead	Digital & SDGE Customer	11/29/2021
16	Domain Architect	Digital & SDGE Customer	11/29/2021
17	Senior Group Product Manager	Digital & SDGE Customer	11/29/2021
18	Product Owner Team Lead	Digital & SDGE Customer	12/6/2021
19	Group Product Manager	Digital & SDGE Customer	12/6/2021
20	Group Product Manager	Digital & SDGE Customer	12/6/2021
21	Demand Response Manager	Customer Programs	12/6/2021
22	Senior Group Product Manager	Cloud & Infrastructure	12/7/2021
23	Group Product Manager	Cloud & Infrastructure	12/7/2021
24	Security Manager	Corporate Security	12/7/2021
25	Security Risk & Compliance Manager	Security Compliance & Executive Services	12/7/2021
26	Special Agent	Corporate Security	12/7/2021
27	Domain Architect – Cybersecurity	Cybersecurity Risk & Compliance	12/7/2021
28	Chief Counsel Technology & Business Services	Technology & Business Services	12/8/2021

#	Title	Organizational Unit	Date
29	Regulatory Compliance Advisor	Enterprise Risk & Compliance	12/9/2021
30	Regulatory Affiliate Compliance Manager	Risk & Compliance	12/9/2021
31	Regulatory Compliance analyst	Risk & Compliance	12/9/2021
32	Managing Attorney	Litigation and Wildfire Mitigation	12/10/2021
33	Senior Paralegal	Litigation and Wildfire Mitigation	12/10/2021
34	Senior Counsel	General Counsel - Regulatory	12/13/2021
35	Regulatory Case Manager – III	CPUC/FERC - Gas	12/13/2021
36	Regulatory Case Manager – II	CPUC/FERC - Gas	12/13/2021
37	Senior Counsel	Regulatory	12/13/2021
38	Regulatory Business Manager	Policy & Proceedings	12/13/2021
39	Customer Services Technology Manager	Customer Operations	12/13/2021
40	Customer Operations Privacy Program Manager	Customer Operations	12/13/2021
41	Portfolio Manager	Supply Management & Div Business Enterprise	12/13/2021
42	Value Capability Manager	Cybersecurity Risk & Compliance	12/13/2021
43	Credit & Collections Supervisor	Customer Operations	12/13/2021
44	Customer Payments Analyst	Customer Operations	12/13/2021
45	Customer Operations Analyst	Customer Operations	12/13/2021
46	Project Manager – II	Gas Engineering	12/13/2021

#	Title	Organizational Unit	Date
47	Team Leader – IV	Customer Field Operations	12/13/2021
48	Smart Meter Capital Project Manager	Customer Field Operations	12/13/2021
49	Customer Services GRC Project Lead	Customer Field Operations	12/13/2021
50	Billing Analyst – I	Customer Operations	12/14/2021
51	Billing Analyst – I	Customer Operations	12/14/2021
52	Senior Market Advisor – I	Customer Operations	12/14/2021
53	CCA Billing Operations Manager	Customer Operations	12/14/2021
54	CCA Strategy & Pol Manager	Customer Operations	12/14/2021
55	Senior Business Services Analyst	Customer Operations	12/14/2021
56	Manager - Customer Care Centers	Customer Care	12/14/2021
57	Customer Billing Manager	Customer Operations	12/15/2021
58	Customer Operations Analytics Supervisor	Customer Operations	12/15/2021
59	Director - Cloud & Infrastructure	Cloud & Infrastructure	12/15/2021
60	Prin Special Agent	Corporate Security	12/15/2021
61	Factories Manager	Support Services - SDG&E	12/15/2021
62	Senior Domain Architect	Digital Workspace & Automation	12/15/2021
63	Director - Digital & SDGE Customer	Digital & SDGE Customer	12/17/2021
64	Scrum Master Team Lead	Digital & SDGE Customer	12/17/2021

#	Title	Organizational Unit	Date
65	Value Capability Manager	Cybersecurity Risk & Compliance	12/17/2021
66	Customer Care Center Operations Strategy Project Manager	Customer Care	1/4/2022
67	Senior Complaint Resolution Advisor	Customer Care	1/4/2022
68	Project Manager - II	Customer Care	1/7/2022
69	Branch Offices Supervisor	Customer Care	1/7/2022
70	Customer Care Centers Operations Manager	Customer Care	1/7/2022
71	IAM Manager	Digital Workspace & Automation	1/7/2022
72	IAM Manager	Digital Workspace & Automation	1/7/2022
73	Senior Domain Architect	Digital Workspace & Automation	1/7/2022
74	Senior Vice President - Customer Service & External Affairs	Customer Services & External Affairs	1/20/2022
75	Director - Customer Operations	Customer Operations	1/20/2022
76	Senior Vice President, Chief Information Officer, and Chief Digital Officer	Senior Vice President, Chief Information Officer, and Chief Digital Officer (Executive Office)	2/1/2022

Contact us

Doron Rotman
Managing Director
408-367-7607
drotman@kpmg.com

Alicia Ortego
Director
415-260-5828
aortego@kpmg.com

Chris Kypreos
Director
415-963-5148
ckypreos@kpmg.com

www.kpmg.com

kpmg.com/socialmedia