Company:	Southern California Gas Company (U 904 G)/San Diego Gas & Electric Company (U 902 M)
Proceeding:	2019 General Rate Case
Application:	A.17-10-007/008 (cons.)
Exhibit:	SCG-227/SDG&E-225

SOCALGAS/SDG&E

REBUTTAL TESTIMONY OF GAVIN WORDEN (CYBERSECURITY)

JUNE 18, 2018

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

TABLE OF CONTENTS

SOCALGAS REBUTTAL TESTIMONY OF GAVIN WORDEN
(CYBERSECURITY)

I. SUMMARY OF DIFFERENCES

Tables GW-1 through GW-4, below, summarize the parties' respective Test Year (TY) 2019 forecasts for Southern California Gas Company (SoCalGas) and San Diego Gas & Electric Company (SDG&E) Cybersecurity activities.

TABLE GW- 1- SoCalGas Total Shared O&M

TOTAL SHARED O&M - Constant 2016 ($000)			
	Base Year 2016	**Test Year 2019**	**Change**
SoCalGas	239	708[1]	469
ORA	239	588	349

TABLE GW- 2- SDG&E Total Shared O&M

TOTAL SHARED O&M - Constant 2016 ($000)			
	Base Year 2016	**Test Year 2019**	**Change**
SDG&E	6,568	7,906	1,338
ORA	6,568	7,906	1,338

TABLE GW- 3- SoCalGas Total Capital

TOTAL CAPITAL - Constant 2016 ($000)					
	2017	**2018**	**2019**	**Total**	**Variance**
SoCalGas	17,844	19,476	22,731	60,051	[redacted]
ORA	6,882	7,201	7,896	21,979	38,072

TABLE GW- 4- SDG&E Total Capital

TOTAL CAPITAL - Constant 2016 ($000)					
	2017	**2018**	**2019**	**Total**	**Variance**
SDG&E	6,146	7,232	5,618	18,996	[redacted]
ORA	1,631	1,815	1,887	5,333	13,663

[1] This amount is incorrectly stated in the Direct Testimony of Mark Loy. See, April 13, 2018, Report on the Results of Operations for San Diego Gas & Electric Company, Southern California Gas Company, Test Year 2019, General Rate Case, Information Technology and Cybersecurity, Ex. ORA-20 (Ex. ORA-20 (Loy)) at 24:4-10.

II. INTRODUCTION

This rebuttal testimony regarding SoCalGas and SDG&E's (collectively, the Companies) request for Cybersecurity costs addresses the following testimony:

- The Office of Ratepayer Advocates (ORA) as submitted by Mr. Mark Loy.[2]

As a preliminary matter, the absence of a response to any particular issue in this rebuttal testimony does not imply or constitute agreement by SoCalGas and/or SDG&E with the proposal or contention made by these or other parties. SoCalGas/SDG&E's direct testimony is based on information known at the time of testimony preparation.

A. ORA

The following is a summary of ORA's position(s):

- A forecast of $588,000 million for shared Operations and Maintenance (O&M) expenses, a reduction of $120,000 from SoCalGas' forecast of $708,000 million.[3]
- Adopt the Adjusted-Recorded amount of $6.882 million for capital expenditures in 2017, a reduction of $10.962 million from SoCalGas' forecast of $17.844 million.[4]
- A forecast of $7.201 million for capital expenditures in 2018, a reduction of $12.275 million from SoCalGas' forecast of $19.476 million.[5]
- A forecast of $7.896 million for capital expenditures in 2019, a reduction of $14.835 million from SoCalGas' forecast of $22.731 million.[6]
- No adjustments to SDG&E's forecast of Cybersecurity O&M expenses.[7]

---

[2] Ex. ORA-20 (Loy).

[3] Ex.ORA-20 (Loy) at 6:9-10.

[4] *Id*. at 6:17-19.

[5] *Id*. at 6:20-21.

[6] *Id*. at 7:1-2.

[7] *Id*. at 5:5-6.

- Adopt the Adjusted-Recorded amount of $1.632 million for capital expenditures in 2017, a reduction of $4.514 million from SDG&E's forecast of $6.146,000.[8]
- A forecast of $1.815 million for capital expenditures in 2018, a reduction of $5.417 million from SDG&E's forecast of $7.232 million.[9]
- A forecast of $1.888 million for capital expenditures in 2019, a reduction of $3.730 million from SDG&E's forecast of $5.618 million.[10]

III. REBUTTAL TO ORA'S O&M PROPOSALS

A. Non-Disputed Cost

ORA takes no issue with the Test Year O&M forecast for SDG&E's Cybersecurity shared costs.

B. Disputed Cost

ORA takes issue with the Test Year O&M forecast for SoCalGas Cybersecurity shared expenses. ORA states that since SoCalGas' 2017 forecast exceeded the 2017 adjusted, recorded expense by 20.5%, the 2018 and 2019 forecasts should be reduced to equal the 2017 adjusted, recorded expense.[11] Put another way, ORA asserts that because SoCalGas only spent $588,000 in 2017 O&M, the California Public Utilities Commission (Commission) should only authorize $588,000 for 2019 O&M.

1. ORA does not dispute SoCalGas' forecasting method

SoCalGas disagrees with ORA's assessment that because SoCalGas spent less than it had forecasted in 2017, the Commission should reduce SoCalGas' forecast for 2019 to the exact same amount as 2017 actuals. As explained in my revised testimony,[12] the forecast methodology utilized by SoCalGas for this cost category is derived from base year (BY) 2016 recorded costs, plus adjustments. This methodology was neither disputed nor challenged by ORA. Instead, ORA proposed a different methodology consisting of actuals from a single year without

---

[8] *Id*. at 5:13-15.

[9] *Id*. at 5:16-17.

[10] *Id*. at 5:18-19.

[11] *Id*. at 24:12-14.

[12] December 2017, Revised SoCalGas Direct Testimony of Gavin Worden (Cybersecurity), Ex. SCG-27-R (SCG-27-R (Worden)) at GW-25:2-4.

considering changes to the operational environment. Utilizing a single year as a forecasting method does not make sense in the context of the cybersecurity operational environment, which does not remain static between fiscal years. The funding requirements relate directly to the number of systems and activities requiring support. When the operational environment has an increase in the number of supported systems and processes there needs to be a corresponding increase in the number of personnel to support these systems and processes. ORA's recommendation does not consider the fact that prior capital projects require O&M funding to support ongoing operations. Additionally, the increase of O&M is in support of risk mitigation activities addressed in the Risk Assessment and Mitigation Plan (RAMP).

2. ORA fails to address or consider RAMP in their proposed O&M forecast

Per the Commission's Decision 14-12-025[13] the California utilities were ordered to "incorporate a risk-based decision-making framework into the Rate Case Plan (RCP) for the energy utilities' General Rate Cases (GRC)." The Companies filed the RAMP on November 30, 2016 identifying "SoCalGas and SDG&E's baseline assessment of safety risks to the public, their employees and their systems, and what potential mitigation measures have been considered. Based on those potential mitigation measures, the utilities then propose certain mitigation measures to further reduce identified risks."[14] Starting in 2017, there were new personnel and contract requirements that directly support these RAMP mitigation efforts, summarized in the table below. These vacant positions require sufficient lead time to staff due to the limited supply of qualified cybersecurity personnel. While new personnel were hired, they were hired midway through 2017; as such, SoCalGas did not utilize all funding allocated, which is why there was a gap between targets and actuals. ORA's recommendation to use the 2017 adjusted recorded expense does not provide sufficient funds to staff a fully functional cybersecurity team required in 2019 and subsequent attrition years to mitigate and address the risks identified within the RAMP report.

[13] Decision (D.) 14-12-025 at 2.

[14] Investigation (I.) 16-10-016, Risk Assessment and Mitigation Phase Report of San Diego Gas & Electric Company and Southern California Gas Company (RAMP Report) (Filed November 30, 2016) at A-1.

IV. REBUTTAL TO ORA'S CAPITAL PROPOSALS

TABLE GW- 8 - SoCalGas GRC Capital Proposals

TOTAL CAPITAL - Constant 2016 ($000)					
	2017	**2018**	**2019**	**Total**	**Variance**
SoCalGas	17,844	19,476	22,731	60,051	
ORA	6,882	7,201	7,896	21,979	38,072

TABLE GW- 9 – SDG&E GRC Capital Proposals

TOTAL CAPITAL - Constant 2016 ($000)					
	2017	**2018**	**2019**	**Total**	**Variance**
SDG&E	6,146	7,232	5,618	18,996	
ORA	1,631	1,815	1,887	5,333	13,663

A. Disputed Costs

ORA recommends adopting the adjusted, recorded 2017 costs as the capital forecast for 2017 and takes issue with subsequent capital forecasts for 2018 and TY 2019. ORA states that because the Companies' 2017 estimates were higher than the 2017 adjusted recorded amount, the 2018 and 2019 forecasts should be adjusted utilizing a least squares time trend, which the Companies understand to be a multi-year trend analysis.[15]

1. ORA's forecasting methodology is flawed

The Companies disagree with the methodology employed by ORA in determining forecast years based upon actuals from a single budget year, or from trending across multiple previous budget years. The Companies utilize a zero-based forecast methodology for Cybersecurity capital costs. Due to the rapidly changing cybersecurity threat environment, this method is most appropriate as these estimates are based upon specific projects, assets, and tasks needed for cybersecurity risk management and mitigation.

Utilizing a multi-year trend analysis to determine capital expenses is not a logical approach to funding capital projects, especially as it relates to necessary expenditures to directly address cybersecurity risks that have been identified via RAMP and on-going risk assessments. Specifically, historical expenditures are not sufficient to address increasing cybersecurity threats, which are constantly emerging in a dynamic environment. ORA did not dispute the use of a zero-based forecast methodology as being appropriate (or challenge the merits of any specific

[15] ORA-20 (Loy) at 25:1-3.

project), but stated that because the Companies did not meet its target for one single year (2017), a multi-year trend analysis based forecast should be used instead. ORA's recommendations to significantly reduce SoCalGas' and SDG&E's Cybersecurity planned capital expenditures make no sense in an environment of increasing cyber threats and risks.

2. ORA fails to address or consider RAMP in their proposed Capital forecast

ORA's recommendation is not consistent with the Commission's directive to incorporate a risk-based framework into the current GRC request. As identified within the RAMP[16] report, cybersecurity risk is a top safety risk for the Companies. The RAMP report was the starting point for consideration of the risk mitigation efforts as defined within my revised testimony. The RAMP report presented an assessment of the key safety risks of SoCalGas and SDG&E and proposed plans for mitigating those risks. As discussed in the direct testimony of Diana Day[17] and Jamie York,[18] the costs of risk-mitigation projects and programs were translated from the RAMP Report into the GRC individual witness areas. As stated in the RAMP report, company subject matter experts used empirical data to the extent available and/or their expertise to determine the likelihood and impact of a cybersecurity incident. The likelihood score was determined as being at least a 4 (Occasional), which is defined in the Risk Evaluation Framework as the possibility of a cybersecurity-related event occurring. The impact scores of the Companies' cybersecurity risks were determined to be at least 5 (Extensive) to a 6 (Severe) depending on the RAMP area. Those assigning this score considered reports in open media, security research, information-sharing entities, contracted information services, and threat intelligence sources. The findings are shown below.

[16] RAMP Report at A-1.

[17] October 6, 2017, Direct Testimony of Diana Day (Chapter 1: Risk Management Policy), Ex. SCG-02/SDG&E-02.

[18] October 6, 2017, Direct Testimony of Jamie York (Chapter 3: RAMP to GRC Integration), Ex. SCG-02/SDG&E-02.

TABLE GW- 10 - RAMP Findings

RAMP Area	Findings
Operational and Reliability	A score of 6 (Severe) was given to this risk. A cyber security incident impacting transmission and/or distribution of energy would directly impact the reliable delivery of energy.
Regulatory, Legal, and Compliance	Cyber Security was scored a 5 (Extensive) in the Regulatory, Legal, and Compliance impact area. This is reasonable because a severe impact to operations would likely result in an extended and in-depth review of the incident, as well as the existing mitigations and activities related to Cyber Security at the time of the event.
Financial	The Financial impact of a cyber security incident was also scored as a 5 (Extensive). A variety of cyber incidents could potentially result in this level of financial impact due to the high visibility of this kind of incident in our industry. A customer information breach may potentially result in reparations, security investigation and improvement costs, and a loss of customer confidence. An energy outage could result in financial impacts, loss of confidence, and/or increased insurance costs. The possibility of an incident destroying assets or data, such as an Advanced Meter Infrastructure (AMI) solution, could also be severe.

3. ORA fails to consider increasing cybersecurity risks

The increasing complexity and frequency of cybersecurity-related attacks require companies to increase their cybersecurity capabilities. There have been multiple large-scale cybersecurity attacks across various industries, including Energy, that have caused disruption of service and loss of company and customer data. Examples include:

- 2012 virus attack on Saudi Aramco which infected 30,000 systems and deleted data from computer hard drives.[19]
- 2015 attack on the Ukrainian Power Grid (UPG) in which power system components were maliciously operated and automation systems were disabled resulting in disruption of power delivery to customers.[20]

[19] Ex. SCG-27-R (Worden) at GW-19, n.12.

[20] *Id.* at GW-19:11-19.

- 2015 attack on the United States Office of Personnel Management (OPM) that released sensitive information associated with 21.5 million people.[21]
- 2016 Yahoo password breach which affected 500 million accounts.[22]
- 2016 Lansing Board of Water and Light ransomware attack that impacted significant numbers of corporate computers.[23]

The United States Computer Emergency Readiness Team (US-CERT) has recently released alerts (TA17-293A, and TA-18-074A) identifying an "Advanced Persistent threat activity targeting Energy and other critical infrastructure sectors."[24] These alerts, coupled with the previously mentioned attacks, show that cybersecurity risk is significant and increasing, potentially impacting the operational integrity of energy delivery systems and sensitive customer and company information. Combatting these threats requires an investment in cybersecurity services, technology, and personnel and the consequences of not treating these threats seriously will put the Companies, the industry, and customers at risk.

V. CONCLUSION

The Companies have addressed the proposed recommendations presented by ORA and demonstrated that ORA's proposals are not warranted. In summary, the Companies have demonstrated the following:

- SoCalGas' TY 2019 shared O&M forecast is reasonable; and
- The Companies' 2018 and TY 2019 capital expenditure forecasts are reasonable.

Accordingly, the Companies' forecasts for TY 2019 Cybersecurity Shared O&M and Capital Expenditure forecasts should be adopted by the Commission.

This concludes my prepared rebuttal testimony.

---

[21] *Id.* at GW-20, n.13.

[22] *Id*. at GW-20, n.14.

[23] *Id.* at GW-19, n.12.

[24] United States Computer Emergency Readiness Team (US-CERT), *Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors* (October 20, 2017), *available at* https://www.us-cert.gov/ncas/alerts/TA17-293A.

APPENDIX A

GLOSSARY OF TERMS

AMI	Advanced Meter Infrastructure
BY	Base Year
CPUC/Commission	California Public Utilities Commission
GRCs	General Rate Cases
I	Investigation
O&M	Operations and Maintenance
OPM	Office of Personnel Management
ORA	Office of Ratepayer Advocates
RAMP	Risk Assessment and Mitigation Plan
RCP	Rate Case Plan
SDG&E	San Diego Gas & Electric Company
SoCalGas	Southern California Gas Company
US-CERT	United States Computer Emergency Readiness Team
TY	Test Year
UPG	Ukrainian Power Grid