Company: Southern California Gas Company (U 904 G)
Proceeding: 2024 General Rate Case
Application: A.22-05-015 /-016 (consolidated)
Exhibit: SCG-222

REBUTTAL TESTIMONY OF

OMAR ZEVALLOS

(CYBERSECURITY)

BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

May 2023

TABLE OF CONTENTS

I. SUMMARY OF DIFFERENCES 1

II. INTRODUCTION 1

A. Cal Advocates 2

III. REBUTTAL TO CAL ADVOCATES O&M PROPOSAL 6

A. Shared Services O&M 6

IV. REBUTTAL TO CAL ADVOCATES' CAPITAL PROPOSAL 6

A. Capital Costs 6

1. Cal Advocates Fails to Account for Proper Asset Allocation and Does Not Acknowledge the Rapidly Evolving Cybersecurity Threat Landscape. 7

2. Cal Advocates Proposed Forecast Methodology is Unsupported and Would Severely Underfund Cybersecurity, Placing SoCalGas's Systems, Infrastructure and Customers at Risk. 9

3. Cal Advocates Recommendation for A Two-Way Balancing Account Would also Limit SoCalGas's Ability to Protect Against Evolving Threats to Cybersecurity. 10

V. CONCLUSION 10

VI. WITNESS QUALIFICATIONS 12

APPENDIX A – GLOSSARY OF TERMS

APPENDIX B – DATA REQUEST RESPONSES

REBUTTAL TESTIMONY OF OMAR ZEVALLOS (CYBERSECURITY)

I. SUMMARY OF DIFFERENCES

TOTAL O&M - Constant 2021 ($000)			
	Base Year 2021	**Test Year 2024**	**Change**
SOCALGAS	3,850	3,936	86
CAL ADVOCATES	3,850	3,936	86

TOTAL CAPITAL - Constant 2021 ($000)					
	2022	**2023**	**2024**	**Total**	**Difference**
SOCALGAS	28,842	36,788	42,915	108,545	
CAL ADVOCATES	20,554	23,570	23,570	67,694	40,851

II. INTRODUCTION

This testimony chapter (1) adopts the direct testimony of Lance Mueller and work papers supporting Southern California Gas Company's (SoCalGas) request for Cybersecurity costs;[1] and (2) addresses the following testimony from other parties:

- The Public Advocates Office of the California Public Utilities Commission (Cal Advocates) as submitted by L. Mark Waterworth (Ex. CA-11), dated March 27, 2023.[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 with the proposal or contention made by these or other parties. The forecasts contained in SoCalGas's prepared direct testimony,

[1] Revised Prepared Direct Testimony of Lance R. Mueller (Cybersecurity) (August 2022) (Exhibit (Ex.) SCG-22-R (Mueller)); Revised Workpapers to Prepared Direct Testimony of Lance R. Mueller on Behalf of Southern California Gas Company (August 2022) (Ex.t SCG-22-WP-R (Mueller)); Revised Capital Workpapers to Prepared Direct Testimony of Lance R. Mueller on Behalf of Southern California Gas Company (August 2022) (Ex. SCG-22-CWP-R (Mueller)).

[2] Public Advocates Office Report on the Results of Operations for Southern California Gas Company and San Diego Gas & Electric Company Test Year 2024 General Rate Case, SCG and SDG&E Supply Management/Logistics & Supplier Diversity, Fleet Services, Real Estate & Facility Operations, Environmental Services, Information Technology, Cybersecurity; and SDG&E Clean Transportation, Exhibit CA-11 (March 27, 2023) (Ex. CA-11 (Waterworth)).

performed at the project level, are based on sound estimates of its revenue requirements at the time of testimony preparation.

Enhancing the cybersecurity posture within SoCalGas will require continued evolution and introduction of modern technologies to enhance or replace aging systems that may add risk to SoCalGas's systems. As discussed in the Cybersecurity testimony (Exhibit SCG-22-R), the five risk areas, Perimeter Defenses, Internal Defenses, Sensitive Data Protection, Operational Technology Cybersecurity, and Obsolete IT Infrastructure Application Replacement, require significant investment to keep up with a rapidly evolving threat landscape.[3] Cybersecurity threats are not static, and the measures taken to mitigate against these threats, by necessity, must continuously change. For example, SoCalGas is witnessing an evolving threat landscape driven by widespread adoption of artificial intelligence, machine learning, and continued digitalization of operational technologies. Adoption of these technologies further stresses the importance of implementing rapid, proactive, and expedient countermeasures against potential threat actors. SoCalGas's request for capital expenditures supports these activities, to mitigate and reduce risk to our business and the communities we serve.

A. Cal Advocates

The following is a summary of Cal Advocates' positions:[4]

- Cal Advocates does not oppose SoCalGas's Test Year Operations & Maintenance (O&M) forecast.
- Cal Advocates recommends an overall $40,851 million reduction from SoCalGas's $108,545 million Test Year (TY) 2024 forecast based on its assertion that SoCalGas has not adequately supported the requested increase in expense over the historical expenses and asserts that SoCalGas provides no explanation as to why its forecast should be proportionately different from SDG&E's.
- Cal Advocates recommends a forecast of $20,554 million for capital expenditures in 2022, which represents a $8,288 million reduction from SoCalGas's forecast of $28,842 million.

[3] Ex. SCG-22-R (Mueller) at LRM-8 – LRM-9.

[4] Ex. CA-11 (Waterworth) at 71 – 82.

- Cal Advocates recommends a forecast of $23,570 million for capital expenditures in 2023, which represents a $13,218 million reduction from SoCalGas's forecast of $36,788 million.
- Cal Advocates recommends a forecast of $23,570 million for capital expenditures in 2024, which represents a $19,345 million reduction from SoCalGas's forecast of $42,915.

As reflected in direct testimony SoCalGas created its capital forecast after thorough review and consideration of current business conditions, cybersecurity industry conditions, and the current threat landscape in the energy and utilities industry.[5] SoCalGas disagrees with Cal Advocate's position that the Cybersecurity capital forecasts are "quantitatively unsupported" overall.[6] SoCalGas also disagrees with Cal Advocates' position that the SoCalGas capital forecast should be based on a 5-year average percentage of capital expenditures in proportion to SDGE's capital expenditures.[7]

Cal Advocates has incorrectly surmised that SoCalGas's capital expenditures should be relatively similar to SDG&E's by failing to recognize that cybersecurity capital assets are a shared asset. The capital costs for a shared asset are recorded on the financial records of the utility that receives the most service or use from the asset and costs are allocated to the other Sempra affiliate(s) based on a utilization factor developed specifically for each forecasted project, as described in SoCalGas's Shared Services prepared direct testimony and workpapers.[8] Computer hardware and software utilization factors are tracked ranging from the number of users to the amount of activity (bandwidth) used for each company, and as such SoCalGas is the primary user of these assets.

As more Operational Technology is adopted and the technology infrastructure that provides key capabilities and services ages, the need to invest in Operational Technology

---

5 Ex. SCG-22-R (Mueller) at LRM-17.

6 Ex. CA-11 (Waterworth) at 4.

7 *Id*. at 80 – 81.

8 Revised Prepared Direct Testimony of Angel N. Le and Paul D. Malin (Shared Services Billing, Shared Assets Billing, Segmentation, & Capital Reassignments) (August 2022) (Ex. SCG-30-R/ SDG&E-34-R (Le and Malin)) at 16 – 21; Revised Workpapers to Prepared Direct Testimony of Angel N. Le and Paul D. Malin on Behalf of Southern California Gas Company and San Diego Gas & Electric Company (August 2022) (Ex. SCG-30-WP/SDG&E-34-WP-R (Le and Malin)).

Cybersecurity and Obsolete IT Infrastructure Application Replacement areas increases. SoCalGas's infrastructure and applications are now reaching their standard upgrade or replacement shelf-life. Software and hardware asset depreciation guidelines are often within a five-year period and/or when the Original Equipment Manufacturer no longer supports or provides security updates. Within that same timeframe, software vendors may also make updates, known as patches, to their technology to address vulnerabilities and known threats. As such, the steady increase of investments in cybersecurity protections at SoCalGas reflects this environment and requires that the Company employ the current, vendor-supported version of applications, while continuously evolving practice, techniques, tools, and capabilities at or faster than the pace of threat actors.

Evolving vulnerabilities in existing systems may also require SoCalGas's capital investment in enhancements, upgrades, or replacements before SoCalGas has fully depreciated those products, but those investments are necessary. Strengthening the defenses of our perimeter, protecting sensitive customer data and enforcing robust internal defenses, are paramount to SoCalGas's cybersecurity operations and the integrity of the Company's systems and protections. Addressing vulnerabilities in systems and applications as expeditiously as possible allows SoCalGas to close or minimize any potential points of entry to threat actors.

Although SoCalGas provided data and the information requested to Cal Advocates – highlighting examples of larger projects within the SoCalGas forecast – Cal Advocates takes the position that it "considers the support lacking because SCG's proof is limited to numbers on a page."[9] This statement is irresponsible and untrue. In addition to its prepared direct testimony, SoCalGas provided responses to Cal Advocates' data requests that discussed the larger projects, which Cal Advocates agreed to, providing details but removing the actual name of the solution. For the three projects that Cal Advocates shares in Table 11-46 of their testimony, SoCalGas had provided additional commentary and details about the submission and associated costs.[10]

[9] Ex. CA-11 (Waterworth) at 80.

[10] *Id.*

For example, for *Project 9* within the SoCalGas response, the following detail was provided:

> Project 9 will deploy an Enterprise Risk Management Solution, including 4 key components within SoCalGas's Enterprise Governance Risk and Compliance system. (1) Corporate Security (2) Corporate SOX (3) Risk Management and (4) Third Party and Vendor Risk Management. Collectively, this system will increase SoCalGas's ability to respond to threats, improve SOX compliance and efficiency, provide a single Risk Management repository, and automate existing third party and vendor risk management processes.
>
> Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors and suppliers. Additional specialized roles for the on-premises product that Sempra currently utilizes is required, such as architects, domain engineers, cybersecurity engineers and analysts can also be included in these costs.
>
> The majority of non-labor costs for this project represent investments to specialized engineering vendor resources, with knowledge of the on-premises solution including its associated capabilities, services and configuration. Hardware costs include initial user licenses, initial implementation support and replacement of current end of support or end of life hardware.
>
> Administrative costs represent a percentage allocate[d] to cover costs incurred to run the project that potentially overlap across utilities (*e.g.*, costs incurred and billed [to] SDG&E by an SoCalGas employee or vice versa).[11]

SoCalGas also offered Cal Advocates a walk-through of the projects, which Cal Advocates accepted and attended. As indicated in its prepared direct testimony, SoCalGas does not disclose sensitive information about its cybersecurity-related controls, intelligence, strategies, and tactics in the public record to avoid aiding adversaries that could disrupt its systems and impede its ability to serve its customers.[12] SoCalGas reiterates its commitment to discuss sensitive details associated with the content of the requests upon Commission request for discussion in person.

---

[11] *See* Appendix B, SoCalGas Response to PAO-SCG-054-LMW, Question 3, attached hereto.

[12] Ex. SCG-22-R (Mueller) at LRM-7 – LRM-8; *See also* Appendix B SoCalGas Response to PAO-SCG-05-LMW, Question 3.

III. REBUTTAL TO CAL ADVOCATES O&M PROPOSAL

Cal Advocates does not oppose SoCalGas's forecast for TY2024 Operations & Maintenance (O&M).

A. Shared Services O&M

SHARED O&M - Constant 2021 ($000)			
	Base Year 2021	**Test Year 2024**	**Change**
SOCALGAS	3,850	3,936	86
CAL ADVOCATES	3,850	3,936	86

IV. REBUTTAL TO CAL ADVOCATES' CAPITAL PROPOSAL

TOTAL CAPITAL - Constant 2021 ($000)					
	2022	**2023**	**2024**	**Total**	**Difference**
SOCALGAS	28,842	36,788	42,915	108,545	
CAL ADVOCATES	20,554	23,570	23,570	67,694	40,851

A. Capital Costs

Cal Advocates takes issue with SoCalGas's capital expenditure forecasts for 2022, 2023 and 2024, stating that the forecasts exceed historical spending, are greater proportionality than SDG&E's cybersecurity capital forecast, and asserting that SoCalGas did s not provide adequate documentation to support the need for increased capital funding. Cal Advocates makes the unfounded statement that SoCalGas requested "an aggressive forecast" because "there are no penalties for requesting more than is reasonable" and recommends a very significant reduction to SoCalGas's capital forecast.[13] Cal Advocates further infers that "[SoCalGas] is attempting to plan for unforeseen needs and increased costs that historical data does not encompass," and then concludes that "unforeseen occurrences is not a valid forecast methodology."[14] SoCalGas disagrees with Cal Advocates' position. Far more than mere numbers on a page, SoCalGas provided in direct testimony, its workpapers and in discovery the reasons for and costs to support the need for increased spending in the Cybersecurity area.[15] With constant reports in the news about cybersecurity breaches and events impacting government, businesses and critical energy

[13] Ex. CA-11 (Waterworth) at 81.

[14] *Id.* at 78.

[15] *See, e.g.,* Appendix B, SoCalGas Response to PAO-SCG-054, Question 3; *see also* Ex. SCG-22-R (Mueller) at Appendix D; *see also* Ex. SCG-22-CWP-R (Mueller) at 26.

infrastructure, SoCalGas takes the ever evolving and sophisticated cybersecurity events seriously, as it must under both state and federal laws, including the Department of Homeland Security and NERC Critical Infrastructure Protection (CIP) requirements. SoCalGas's TY2024 GRC request reflects that it has planned for and anticipates increased and very real cyberthreats over the next four years. In its prepared direct testimony SoCalGas provided examples of recent cyber-attacks at the Ukrainian Power Grid, Colonial Pipeline and First Energy that have proven very damaging to utilities and the customers they serve.[16] SoCalGas also provided examples of how the cybersecurity threat landscape is evolving at a rapid pace and has demonstrated how and why its cybersecurity posture must evolve at a similar rapid pace to protect its assets, infrastructure and customers.

1. Cal Advocates Fails to Account for Proper Asset Allocation and Does Not Acknowledge the Rapidly Evolving Cybersecurity Threat Landscape.

SoCalGas disagrees with Cal Advocates' position that increased cybersecurity investments are unsupported. As stated above, in its prepared direct testimony SoCalGas provided ample examples of breaches of cybersecurity systems that impacted utility infrastructure and the evolving nature of cyber threats. Cal Advocates took "a 5-year average of historical costs comparing SCG's historic expenditures to that of SDG&E's to determine the extent to which SCG spends more than SDG&E,"[17] and derived a 144% variance year-over-year between SDG&E and SoCalGas that it then applied to create its recommended capital forecast for SoCalGas.[18] This logic is entirely flawed and rests on an incorrect premise. As discussed above, Cal Advocates failed to consider the Companies' shared asset allocation, which makes Cal Advocates comparative approach inappropriate. A historical view of expenditures also does not take into consideration "[t]he pace of change in the cybersecurity industry" and evolving nature of cyber threats, which requires increased defenses to combat new and growing cybersecurity events.[19] SoCalGas's decision to use a zero-based forecast methodology is to ensure a more accurate indicator of future costs, that allows for a continuous review of project

[16] Ex. SCG-22-R (Mueller) at LRM-2.

[17] Ex. CA-11 (Waterworth) at 80.

[18] *Id.* at 80 – 81 and Table 11-47.

[19] Ex. SCG-22-R (Mueller) at LRM-17 – LRM-18.

costs, including consideration to scope, schedule and resources (labor and non-labor) at current market quotes and industry conditions.[20]

SoCalGas continues to protect against ever-changing tactics and automated attacks driven by new technologies. In addition to widely used automation, recent studies show that users' interaction with artificial intelligence (AI) technologies[21] poses a far greater threat to cybersecurity and society than can currently be anticipated. An illustration of these rapidly evolving threats is the accelerated adoption of AI tools from Q4 2022 through early 2023. Generative AI technologies have demonstrated the capability to decipher common passcodes and login techniques, including adapting to reCAPTCHA security, which is used by government, utility companies and other businesses to validate human interaction with an application login page.[22]

ChatGPT, a popular natural language processing tool that responds in human-like conversation provides another example of emerging threats that require new cybersecurity measures. Threat actors are exploiting the popularity of ChatGPT by luring victims into using or installing malicious software on sensitive devices, such as employee cell phones or laptops, in order to install malware or steal login credentials.

And human error can occur, resulting in a customer or employee unknowingly providing access to internal systems or inadvertently exposing sensitive information and details about our energy infrastructure. Industries, such as energy and utilities, must be prepared to respond to and contain any potential access of information that allows a threat actor to act maliciously within our environment, especially from evolving threats such as those mentioned above. SoCalGas proposed cybersecurity investments at levels that reasonably allow it to keep up with rapidly evolving threats, continue investments across our key risk areas, and enable robust, industry-standard cybersecurity capabilities that provide needed protection to the Company's systems,

---

[20] *Id*. at LRM-19.

[21] *See* CNBC, Artificial Intelligence is Playing a Bigger Role in Cybersecurity, but the Bad Guys May Benefit the Most (September 13, 2022), *available at* https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html.

[22] *See* Independent, No, I'm Not a Robot: ChatGPT Successor Tricks Worker into Thinking it is Human (March 15, 2023), *available at* https://www.independent.co.uk/tech/chatgpt-gpt4-ai-openai-b2301523.html.

infrastructure and its customers. A steady state forecast, as is recommended by Cal Advocates, is insufficient, and imprudent, for an environment and threats that are anything but steady state.

2. Cal Advocates Proposed Forecast Methodology is Unsupported and Would Severely Underfund Cybersecurity, Placing SoCalGas's Systems, Infrastructure and Customers at Risk.

As stated above, Cal Advocates fails to consider proper asset allocation and bases their recommendation on a percentage-based calculation between SDG&E and SoCalGas. SoCalGas's forecasts were developed using a zero-based forecast methodology based on prudent consideration of current best practices and future changes to cyber risks and threats driven in response to future threats from hostile agents and threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes.[23] Cal Advocates does not dispute SoCalGas's assessment of the growing risk of cyber threats. However, Cal Advocates recommends a forecast based on a derived 5-year average of historical expenditures for the illogical reason that SoCalGas has spent more than SDG&E, and Cal Advocates does not understand why.[24]

According to Cal Advocates, there is no justification for proportionate differences between SoCalGas's cybersecurity forecast and SDG&E's forecast, stating, "[b]oth companies are sponsored by the same witness and both companies operate under the same parent corporation in a similar IT environment with similar risks."[25] Cal Advocates statement is misinformed. The allocation of capital expenditures are planned and governed within a capital planning and business case methodology that drives how investments are allocated amongst and within operating companies as was clearly described in both the Cybersecurity prepared direct testimony[26] and the Shared Services prepared direct testimony.[27] A cost-sharing mechanism is factored for any project that will be utilized across SoCalGas, SDG&E, and/or Sempra Corporate

---

[23] Ex. SCG-22-R (Mueller) at LRM-19 – LRM-21.

[24] Ex. CA-11 (Waterworth) at 78 and 80 – 81.

[25] *Id.* at 78.

[26] Ex. SCG-22-R (Mueller) at LRM-3. SoCalGas also identified to Cal Advocates in discovery responses that SoCalGas bore the larger portion of shared capital costs due to its "broader service area and larger user base, therefore the capital project cost allocations on shared assets are greater as compared to SDG&E." *See* Appendix B, SoCalGas Response to PAO-SCG-054-LMW, Question 3 at 7, n.3.

[27] Ex. SCG-30-R/SDG&E-34-R (Le and Malin) at ANL/PDM-21.

Center based on a utilization factor. Not only is Cal Advocates' recommended reduction not justified, but it is imprudent. Cal Advocates' recommended forecast would inhibit investments required to address the evolving and growing cybersecurity threats, add risk to the business and endanger the utility's technology infrastructure.

3. Cal Advocates Recommendation for A Two-Way Balancing Account Would also Limit SoCalGas's Ability to Protect Against Evolving Threats to Cybersecurity.

Cal Advocates recommends, as an alternative to its recommended capital forecast, that SoCalGas be ordered to record cybersecurity costs in a two-way balancing account funded at $20 million per year.[28] Cal Advocates offers no supporting analysis or justification for either the balancing account or the $20 million per year cap recommendations.[29] SoCalGas disagrees with Cal Advocates' recommendations. An annual spending cap suggests that Cal Advocates believes the threat of cybersecurity risk is not increasing and remains static, in contradiction to recent history and expert opinion that demonstrates cyber threats are increasing and that the perpetrators are becoming more and more sophisticated.[30] Adoption of a two-way balancing would create added risk to the business and to the communities we serve, by significantly underfunding SoCalGas's cybersecurity investments and limiting SoCalGas's ability to protect against the evolving threats. Cybersecurity threats require vigilance and proactive actions. SoCalGas's Capital forecast was proposed at a level to permit SoCalGas to develop and deploy robust countermeasures at a faster pace than its adversaries can. For the reasons stated above, SoCalGas requests the Commission reject Cal Advocates' position and adopt SoCalGas's forecast as reasonable.

V. CONCLUSION

SoCalGas demonstrated that Cal Advocates' proposals are unwarranted and unsuitable for the current cybersecurity threat landscape faced by SoCalGas and the energy and utilities industries as a whole. SoCalGas must prudently strengthen its cybersecurity defenses, not weaken them, as Cal Advocates recommendations would achieve. SoCalGas has demonstrated that:

---

[28] Ex. CA-11 (Waterworth) at 81.

[29] *Id*.

[30] Ex. SCG-22-R (Mueller) at LRM-13 – LRM-14.

- SoCalGas's TY 2024 O&M forecast is reasonable; and
- SoCalGas's 2022, 2023 and TY 2024 capital expenditure forecasts are reasonable.

This concludes my prepared rebuttal testimony.

VI. WITNESS QUALIFICATIONS

My name is Omar Zevallos. My business address is 8680 Balboa Ave., San Diego, CA 92123. My title is Director, Network & Cybersecurity Technology Services. As the Director of Network & Cybersecurity Technology Services, I am responsible for overseeing all aspects of these critical services across SDG&E, SoCalGas, and Corporate Center.

Previous to my current role, I have had leadership positions including Field Engineer, Operations and Engineering Manager for Electric Regional Operations, Manager of Energy Management Systems, Manager of OT Networks, and Sr. Group Product Manager. I am also a US Navy veteran and a licensed Professional Engineer in the State of California.

I am a graduate of San Diego State University, where I earned a Bachelor of Science in Electrical Engineering, and Norwich University, where I received a Master of Science Degree in Organizational Leadership.

I have not previously testified before the Commission.

APPENDIX A

GLOSSARY OF TERMS

ACRONYM	DEFINITION
ChatGPT	Chat Generative Pre-training Transformer (a general-purpose chatbot that uses artificial intelligence to generate text after a user enters a prompt.)
Commission	California Public Utilities Commission
D.	Decision
GRC	General Rate Case
IT	Information Technology
SDG&E	San Diego Gas & Electric Company
SoCalGas	Southern California Gas Company
TY	Test Year

APPENDIX B
DATA REQUEST RESPONSES

PAO-SCG-054-LMW, Question 3, response submitted on 10/26/22.

Data Request Number: PAO-SCG-054-LMW

Proceeding Name: A2205015_016 - SoCalGas and SDGE 2024 GRC

Publish To: Public Advocates Office

Date Received: 10/3/2022

Date Responded: 10/26/2022

3. Pursuant to PAO-SCG-039-LMW Q.4a, Cal Advocates asked for cost support and was provided a one-page response that is nothing more than numbers on a page attempting to justify over $83 million in capital costs from 2022 to 2024.

Per SCG's response above, the information provided did not answer the question relative to "cost support" and again are only unsupported numbers in a table. The numbers provided offer a level of detail that breaks down the amount/cost forecasted helping Cal Advocates better understand the composition of the costs but again does not support the derivation of the amount. Based on this, please provide an explanation (inclusive of any calculations) for each year from 2022 to 2024 showing and supporting how each of the forecasted cost component (e.g. hardware, software, vendor services, and labor) was derived.

If the extent of SCG support for the derivation of its 2022 to 2024 forecast is fully presented within its testimony, workpapers, and data responses (available to Cal Advocates) please confirm this is the full extent of SCG supporting its 2022 - 2024 forecast, and SCG has no other support for the determination of its forecast.

If SCG has additional support, please provide that support in addition to the support already requested. If SCG is still unclear what Cal Advocates is requesting, please contact the witness (in a timely manner prior to answering) to assist in a clearer understanding.

SoCalGas Response 3:

Per discussion on October 7, 2022, with PAO analyst, Mark Waterworth, this question is requesting cost support and more information for the activity areas with "large" increases year-over-year. These activity areas include Perimeter Defenses, Operational Technology (OT) Cybersecurity, Obsolete Information Technology (IT) Infrastructure and Application Replacement. As discussed with Mr. Waterworth, in order to provide more details on the capital forecasting process, the response below details certain projects (highlighted below) in 2022 with cost support. Note, the project names are not provided as a security precaution due to the nature of Cybersecurity threats.

Activity Area	**2022 Project**	**2022** ($ in mil)
Perimeter Defenses		
	Project 1	0.4
	Project 2	0.6
	Project 3	2.6
	Project 4	1.4
Perimeter Defenses Total		**4.9**
Internal		

Defenses		
	Project 5	0.4
	Project 6	2.4
	Project 7	1.7
	Project 8	1.8
	Project 9	3.0
	Project 10	1.0
	Project 11	2.3
	Project 12	1.5
	Project 13	1.5
Internal Defenses Total		**15.6**
Sensitive Data Protection		
	Project 14	0.1
	Project 15	2.6
	Project 16	0.7
	Project 17	0.5
	Project 18	1.5
	Project 19	0.5
	Project 20	1.7
Sensitive Data Protection Total		**7.6**
Operational Technology (OT) Cybersecurity		
	Project 21	0.8
Operational Technology Cybersecurity Total		**0.8**
Cybersecurity Total (2022)		**$28.9**

Reflected in the table above are key projects and their investments aligned to each risk area in 2022. These projects and initiatives implement or enhance new products, enhance or replace existing capabilities, and allow the utility to engage with highly specialized skillsets and experience provided through various vendor services.

Areas that were of notable investment included SoCalGas's cloud security strategy, network security enhancements, and Identity and Access Management (IAM)

capabilities. In order to support the cloud transition,[1] investments in security are required to develop a modern cloud security posture, use automated enforcement of security standards throughout the software development lifecycle, and replace existing on-premises capabilities by placing them in the cloud further removing dependencies within the cloud environments.

Below is a sampling of 5 projects represented in 2022 investments including a cost breakdown and description. Costs are represented in thousands and prior to rounding. Specific solutions, products and applications are purposely not named due to sensitivity of capabilities.

Project 3	
Internal Labor	$259
Non-Labor	$2,211
Administrative	$68
Total	**$2,538**
Rounded to $2.6m	

Project 3 scope will introduce preventative controls allowing Sempra's wired access to act like Sempra's current wireless access. In addition to providing network access based upon Sempra policy; we will also look to integrate this solution with existing cybersecurity investments to automatically remediate malicious or high-risk endpoints while providing visibility and situational awareness to Sempra's network operations center and security operations center.

Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors and suppliers. Additional specialized roles such as architects, domain engineers, cybersecurity engineers, and analysts can also be included in these costs.

The majority of non-labor costs for this project represent investments to cover install, configuration, and testing of hardware and software that enhances network monitoring capabilities. Hardware costs include initial user licenses, initial implementation support, and replacement of current end of support or end of life hardware.

Administrative costs represent a percentage allocated to cover costs incurred to run the project that potentially overlap across utilities (e.g., costs incurred and billed SDG&E by an SoCalGas employee or vice versa).

Project 6	

[1] The cloud transition is further discussed in the Information Technology testimony (Exhibit SCG-21, Chapter 1)

Internal Labor	$179
Non-Labor	$1,976
Administrative	$282
Total	**$2,437**
Rounded to $2.4m	

Project 6 implements privileged access controls for 520 applications within Sempra. Privileged Account Security or Privileged Account Management (PAM) is a mechanism that safeguards identities with special access, further strengthening internal defenses, and sensitive data protection, reducing threats.

Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors and suppliers. Additional specialized roles for the on-premises product that Sempra currently utilizes is required, such as architects, domain engineers, cybersecurity engineers, and analysts can also be included in these costs.

The majority of non-labor costs for this project represent investments to specialized engineering vendor resources, with knowledge of privileged account management tools, capabilities, services and configuration. Hardware costs include initial user licenses, initial implementation support and replacement of current end of support or end of life hardware.

Administrative costs represent a percentage allocate to cover costs incurred to run the project that potentially overlap across utilities (e.g., costs incurred and billed SDG&E by an SoCalGas employee or vice versa).

Project 9	
Internal Labor	$428
Non-Labor	$2,068
Administrative	$159
Total	**$2,655**
Rounded to $3m	

Project 9 will deploy an Enterprise Risk Management Solution, including 4 key components within SoCalGas's Enterprise Governance Risk and Compliance system: (1)

Corporate Security, (2) Corporate SOX, (3) Risk Management, and (4) Third Party and Vendor Risk Management. Collectively, this system will increase SoCalGas's ability to respond to threats, improve SOX compliance and efficiency, provide a single Risk Management repository, and automate existing third party and vendor risk management processes.

Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors and suppliers. Additional specialized roles for the on-premises product that Sempra currently utilizes is required, such as architects, domain engineers, cybersecurity engineers, and analysts can also be included in these costs.

The majority of non-labor costs for this project represent investments to specialized engineering vendor resources, with knowledge of the on-premises solution including its associated capabilities, services and configuration. Hardware costs include initial user licenses, initial implementation support and replacement of current end of support or end of life hardware.

Administrative costs represent a percentage allocate to cover costs incurred to run the project that potentially overlap across utilities (e.g., costs incurred and billed SDG&E by an SoCalGas employee or vice versa).

Project 11	
Internal Labor	$311
Non-Labor	$1,885
Administrative	$60
Total	**$2,256**
Rounded to $2.3m	

Project 11 scope includes replacement of current antivirus products while adding additional, augmented capabilities to other in-house products that modernize SoCalGas's detective, preventative and mitigation techniques on Sempra's user devices and servers that house sensitive information.

Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors, and suppliers. Additional specialized roles such as architects, domain engineers, cybersecurity engineers, and analysts can also be included in these costs.

Data Request Number: PAO-SCG-054-LMW

Proceeding Name: A2205015_016 - SoCalGas and SDGE 2024 GRC

Publish To: Public Advocates Office

Date Received: 10/3/2022

Date Responded: 10/26/2022

Non-labor costs for this project represent use of specialized vendor skillsets, typically with knowledge of antivirus and EDR ("endpoint detection response") capabilities. Additional non-labor costs represent investments to cover install, configuration, and testing of hardware and software that houses the antivirus products.

Administrative costs represent a percentage allocate to cover costs incurred to run the project that potentially overlap across utilities (e.g., costs incurred and billed SDG&E by an SoCalGas employee or vice versa).

Project 15	
Internal Labor	$259
Non-Labor	$2,211
Administrative	$68
Total	$2,538
Rounded to $2.6m	

Project 15 scope includes expanding and enhancement of the current data loss prevention tool to monitor outbound network traffic from applications (data leaving the Sempra network). This will be needed to satisfy required modernization, enhancements to current capabilities and further enabling sensitive data protection.

Internal labor costs provide the necessary project or product management roles to lead, and orchestrate across various teams, vendors, and suppliers. Additional specialized roles such as architects, domain engineers, cybersecurity engineers and analysts can also be included in these costs.

Non-labor costs for this project represent use of specialized vendor skillsets, typically with knowledge of SoCalGas′s current DLP tool. Additional non-labor costs represent investments on hardware and software and software

Administrative costs represent a percentage allocate to cover costs incurred to run the project that potentially overlap across utilities (e.g., costs incurred and billed SDG&E by an SoCalGas employee or vice versa).

Between 2021-2022, SoCalGas has continued to implement cybersecurity capabilities that further strengthen the activity areas Perimeter Defenses, Internal Defenses and Sensitive Data Protection. An example of new capabilities being introduced are cybersecurity penetration testing tools, which enable cybersecurity teams to continuously evaluate security of systems and simulate attack activities in effort to identify vulnerabilities that may be exploited.

Beginning in 2022, the organization has implemented strategies to further separate and protect Operational Technologies (OT) from traditional IT infrastructure in accordance

with regulatory guidance.[2] This guidance comes from Federal and State agencies (e.g., CPUC, CISA, DHS, FERC, TSA, and DOE), responsible for regulating and setting security standards for companies to emphasize the ever-increasing threat level posed by cybersecurity attackers. The evolving regulatory security standards issued by these agencies impact both SoCalGas's O&M and Capital forecasts[3] by driving changes in security systems requirements, design, and enhanced security controls and processes.

One example of a new cybersecurity regulation within our gas control business area is the 2021 Transportation Security Administration (TSA) Security Directive Pipeline-2021-02.2 To mitigate this evolving risk and comply with the numerous regulatory mandates pertaining to cybersecurity, increased O&M costs are necessary to cover labor and non-labor costs necessary to maintain prior investments, revised policy for maintenance of capital projects as well as for additional headcount to implement, support, operate and manage improvements made through capital projects.

The estimated costs across each activity area represent non-labor and labor estimated at 90%/10%, respectively. Non-labor capital costs for this category are primarily for the hardware and software materials for cybersecurity systems and contractor services. The labor capital costs for this category are for the employees assigned to design, build, and deploy the new systems.

[2] *See, e.g.*, California Consumer Privacy Act (CCPA), Sarbanes-Oxley (SOX), CPUC Affiliate Transactions Compliance and other CPUC Privacy Decisions, CA Breach Notification (Cal. Civ. Code §§ 1798.81.5, 1798.82), Identity Theft Prevention (Federal Trade Commission "Red Flag Rules"), State and Federal Retention and eDiscovery, among others.

[3] Note, SoCalGas has a broader service area and larger user base, therefore the capital project cost allocations on shared assets are greater as compared to SDG&E.