Company: Southern California Gas Company (U 904 G) / San Diego Gas & Electric Company (U 902 M)
Proceeding: 2028 General Rate Case
Application: A.26-06-____
Exhibit: SCG-11 / SDGE-15

PREPARED DIRECT TESTIMONY OF OMAR ZEVALLOS

(CYBERSECURITY)

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

June 2026

TABLE OF CONTENTS

I. INTRODUCTION 1
A. Summary of Cybersecurity Costs and Activities 1
B. Increasing Attacks on Energy Infrastructure 6
C. Adversarial Nation-States and Criminal Actors Continue to Pose Immense Cyber Risk 8
D. Role of Artificial Intelligence 15
E. Overall Cost Drivers 16
F. Organization of Testimony 19
G. Support To and From Other Witnesses 19
II. AFFORDABILITY & EFFICIENCY 19
III. NON-SHARED O&M COSTS 20
A. Non-Shared Cybersecurity O&M – SDG&E and SoCalGas 21
1. Forecast Method 22
2. Perimeter Defenses 22
3. Internal Defenses 23
4. Sensitive Data Protections 24
IV. SHARED O&M COSTS 26
A. Shared Cybersecurity – SDG&E and SoCalGas 27
B. Cybersecurity Functional Groups 27
C. Cybersecurity Strategy, Portfolio and Governance 27
D. Cybersecurity Threat Detection & Response 27
E. Cybersecurity Operations & Compliance 28
F. Cybersecurity Architecture & Engineering 28
G. Enterprise Identity Services 28
H. Insider Trust and Forensics 28
1. Forecast Method 29
2. Perimeter Defenses 30
3. Internal Defenses 31
4. Sensitive Data Protection 33
V. RAMP INTO GRC – O&M 35
A. Description of RAMP Mitigations 35
B. Description of Selection and Prioritization of RAMP Risk Mitigations 35
VI. CAPITAL 36

A. SDG&E & SoCalGas 39
1. Forecast Method 39
2. Perimeter Defenses 40
3. Internal Defenses 43
4. Sensitive Data Protections 46
5. Operational Technology (OT) Cybersecurity 49
6. Infrastructure and Platforms Security Lifecycle Management 52
7. Emerging Threat Defenses 56
VII. RAMP INTO GRC - CAPITAL 60
A. Description of RAMP Mitigations 60
B. Description of Selection and Prioritization of RAMP Risk Mitigations 61
VIII. RISK ASSESSMENT MITIGATION PHASE (RAMP) INTEGRATION 63
A. GRC Risk Controls/Mitigations and Benefit Cost Ratios 63
B. Justification for Proposed Mitigations With BCRs <1 64
C. Changes from 2025 RAMP Report 64
D. Feedback from Safety Policy Division and Parties 65
IX. CONCLUSION 67
X. WITNESS QUALIFICATIONS 68

APPENDICES
Appendix A – Glossary of Terms A-1
Appendix B – Glossary of Definitions B-1
Appendix C – Controls and Mitigations Compliance Driver Roadmap C-1
Appendix D – Capital Expenditures D-1
Appendix E – GRC – RAMP Integration E-1
Appendix F – Glossary of Figures F-1
Appendix G – Glossary of Tables G-1

SUMMARY

SDG&E CYBERSECURITY (In 2025 $)			
Categories of Management	***2025 Adjusted-Recorded (000s)***	***TY2028 Est. (000s)***	***Change (000s)***
Total Non-Shared Services	*1,385*	*1,322*	*-63*
Total Shared Services (Incurred)	*10,566*	*12,396*	*1,830*
Total O&M	***11,951***	***13,718***	***1,767***

SDG&E CYBERSECURITY (In 2025 $)							
Categories of Management	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
Total CAPITAL	**32,504**	**0**	**8,690**	**33,818**	**4,661**	**31,457**	**24,935**

SCG CYBERSECURITY (In 2025 $)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Non-Shared Services	2,398	2,343	-55
Total Shared Services (Incurred)	4,200	6,493	2,293
Total O&M	**6,598**	**8,836**	**2,238**

SCG CYBERSECURITY (In 2025 $)							
Categories of Management	**2025 Adjusted-**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**

	Recorded (000s)						
Total CAPITAL	**83,489**	**49,372**	**51,048**	**103,012**	**65,486**	**88,192**	**121,099**

Summary of Requests

- To address cybersecurity risks, SoCalGas and SDG&E must continue to modernize cybersecurity tools and technologies, maintain a highly skilled cybersecurity workforce, and implement adaptive processes capable of responding to evolving attack methods. Cybersecurity activities are essential to protecting critical infrastructure, securing customer and employee data, and complying with increasingly prescriptive state and federal privacy and security requirements. By performing these activities, cybersecurity technology and services directly contribute to the Companies' ability to provide safe, secure, reliable, and affordable service to customers while maintaining a safe work environment for employees.
- Cybersecurity activities are necessary to address an evolving threat environment in which cyber risks continue to increase in complexity, frequency, and sophistication, including risks to critical infrastructure, operations, and sensitive information.
- As critical infrastructure providers, SoCalGas and SDG&E manage enterprise-wide cybersecurity risks across information technology (IT) and operational technology (OT) environments, where a successful cyber incident could impact safety, reliability, and continuity of service.
- Cybersecurity investments support compliance with applicable state and federal security and privacy requirements while enabling continued use of technology to enhance customer service, system capabilities, and operational efficiency.
- The Companies request Commission approval of total Test Year 2028 cybersecurity costs of $22.554 million in operations and maintenance and $136.830 million in capital, as summarized in this chapter, to support enterprise-wide cybersecurity risk mitigation activities.

PRPARED DIRECT TESTIMONY OF OMAR ZEVALLOS (CYBERSECURITY)

I. INTRODUCTION

A. Summary of Cybersecurity Costs and Activities

My testimony supports the Test Year (TY) 2028 forecasts for operations and maintenance (O&M) costs for both non-shared and shared services, and capital costs associated with Cybersecurity for Southern California Gas Company (SoCalGas) and San Diego Gas & Electric Company (SDG&E) (collectively, the Companies). Table OZ-1 summarizes my sponsored costs.

Certain forecasted activities and estimated costs were presented previously in SoCalGas and SDG&E's 2025 RAMP Application 25-05-010/013 (consolidated) filed on May 15, 2025. Those activities and any changes that have occurred since the RAMP filing are detailed in Section VI below.[1]

TABLE OZ-1
Test Year 2028 Summary of Total Costs

SDG&E CYBERSECURITY (In 2025 $)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Non-Shared Services	1,385	1,322	-63
Total Shared Services (Incurred)	10,566	12,396	1,830
Total O&M	**11,951**	**13,718**	**1,767**

[1] California Public Utilities Commission (CPUC), *Safety Policy Division Evaluation Report on Sempra's 2025 RAMP Applications (A.)25-05-010* (October 10, 2025), *available at:* https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/safety-policy-division/reports/safety-policy-division-evaluation-report-on-sempras-2025-ramp-applications.pdf.

SoCalGas CYBERSECURITY (In 2025 $)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Non-Shared Services	2,398	2,343	-55
Total Shared Services (Incurred)	4,200	6,493	2,293
Total O&M	**6,598**	**8,836**	**2,238**

1

SDG&E CYBERSECURITY (In 2025 $)							
Categories of Management	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
Total CAPITAL	**32,504**	**0**	**8,690**	**33,818**	**4,661**	**31,457**	**24,935**

2

SoCalGas CYBERSECURITY (In 2025 $)							
Categories of Management	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
Total CAPITAL	**83,489**	**49,372**	**51,048**	**103,012**	**65,486**	**88,192**	**121,099**

Companies currently operate in an environment where cybersecurity[2] threats are constant and continue to grow in complexity, frequency, and sophistication. In addition to traditional phishing[3], social engineering[4], and vulnerability[5] exploitation, adversaries are increasingly leveraging emerging technologies such as artificial intelligence (AI)[6] and deepfake[7] capabilities to automate attacks, identify unknown system vulnerabilities[8], impersonate trusted individuals, and undermine the integrity of digital communications and systems. In addition, the potential for future advances in quantum computing[9] to compromise widely used cryptographic standards (e.g., password and information protection) introduces long-term risks that require proactive detection and mitigation planning and investment.

As critical infrastructure organizations, SoCalGas and SDG&E face significant risks from highly sophisticated threat actors.[10] Nation-state adversaries continue to pose one of the highest and most persistent cyber risks to the utility industry. At the same time, the expansion of

---

[2] Cybersecurity: the protection of information technology and operational technology systems, networks, and data from unauthorized access, disruption, or malicious activity.

[3] Phishing: deceptive attempts to obtain sensitive information by impersonating trusted entities through electronic communications.

[4] Social Engineering: techniques used to manipulate individuals into disclosing confidential information or performing actions that compromise security.

[5] Vulnerability: a weakness in systems, processes, or controls that may be exploited by a threat actor.

[6] Artificial Intelligence: technologies used to enhance threat detection and response; additionally describes tools used by threat actors to automate attacks and generate deceptive content.

[7] Deepfake: artificially generated content used to impersonate individuals or manipulate communications for malicious purposes.

[8] PCMag, *Companies Using Anthropic's Mythos AI Uncover 10K+ Serious Software Vulnerabilities*, *available at:* https://www.pcmag.com/news/companies-using-anthropics-mythos-ai-uncover-10k-plus-serious-software.

[9] Quantum Computing: a form of computing that uses quantum-mechanical principles to process information and may pose future cybersecurity risks by compromising existing cryptographic methods.

[10] Threat Actor: an individual or group that conducts or attempts to conduct cyberattacks against systems or infrastructure.

distributed energy resources (DER),[11] cloud-based platforms,[12] network connected remotely controllable devices and operational technology[13] has significantly increased potential attack surface[14] for utilities. A successful cybersecurity attack could introduce potential safety issues, significantly disrupt critical business functions, impair energy delivery to government, commercial, industrial, and residential customers, and/or compromise sensitive customer or employee information.

The Cybersecurity department is responsible for cybersecurity risk mitigation for information and operational technologies (IT and OT) for SoCalGas, SDG&E, and Sempra Energy Corporate Center (Sempra or Corporate Center). As highlighted in the Information Technology testimony (Ex. SCG-10/SDGE-14), SoCalGas and SDG&E are continuing the transition to digital-focused technologies, with added emphasis on shifting applications to the cloud, investing in foundational technology that can make workers more productive, and carefully managing technology lifecycles. Cybersecurity is part of this transition and is a critical component of proactively mitigating risk. The focus of Cybersecurity is maintaining and improving the Company's security posture in an environment of increasing threat velocity and capabilities. Cybersecurity continues to enable technology innovations and enhancements within the business by reducing both the likelihood and potential impact of cybersecurity incidents[15] to all business areas within SoCalGas, SDG&E, and Corporate Center while optimizing cost efficiency through prioritized, risk-based decision-making.

---

[11] Distributed Energy Resources (DERs): small-scale energy systems that generate, store, or manage electricity close to where it is used. DERs include technologies such as rooftop solar panels, battery storage systems, electric vehicles, and demand-side management programs. These systems can be connected to electric grids or isolated, with energy flowing only to specific sites or functions.

[12] Cloud-Based Platforms: systems and applications hosted in cloud environments that support operations, data storage, and system functionality.

[13] Operational Technology: hardware and software used to monitor and control physical processes, including gas and electric system operations.

[14] Attack Surface: the total set of digital, physical, and human-facing entry points through which an unauthorized party could attempt to access, disrupt, or extract data from an organization's systems.

[15] Cybersecurity Incident: an event that may disrupt operations, compromise systems, or result in unauthorized access to data or infrastructure.

Federal and state agencies[16] responsible for regulating and setting security standards for companies continue to emphasize the ever-increasing threat level posed by cybersecurity attackers. For example, in 2026, the White House published a presidential Cyber Strategy for America, reaffirming the designation of the energy grid as critical infrastructure and one of six cyber priorities for the country. The National Cyber Strategy emphasizes the criticality of hardening cybersecurity infrastructure in the Companies' sector and securing information and operational technology supply chains.[17]

Evolving regulatory and contractual security standards include enforceable mandates, such as TSA security requirements and, where applicable, Department of Defense's Defense Federal Acquisition Regulation Supplement (DFARS)[18] requirements governing the handling and protection of Controlled Unclassified Information (CUI), which require defined cybersecurity activities including risk assessments, control implementation, monitoring, documentation, and audit readiness.

In some cases, regulations require utilities to perform specific activities, such as cybersecurity risk assessments[19], incident reporting, and audit preparation. In other cases, they establish minimum security expectations or thresholds, such as requirements for access controls, monitoring, logging, and incident response[20] capabilities, while allowing utilities discretion in how those outcomes are achieved. Together, these mandates impact O&M and capital forecasts by driving changes in security system requirements, design, and implementation of updated security controls and processes.

---

[16] Federal and state agencies include: CPUC, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), Federal Energy Regulatory Commission (FERC), Transportation Security Administration (TSA), and Department of Energy (DOE).

[17] The White House, *President Trump's Cyber Strategy for America* (March 2026), *available at:* https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[18] DFARS establishes cybersecurity requirements for entities performing work under U.S. Department of Defense contracts, including protection of Controlled Unclassified Information (CUI) and implementation of NIST SP 800-171 security controls.

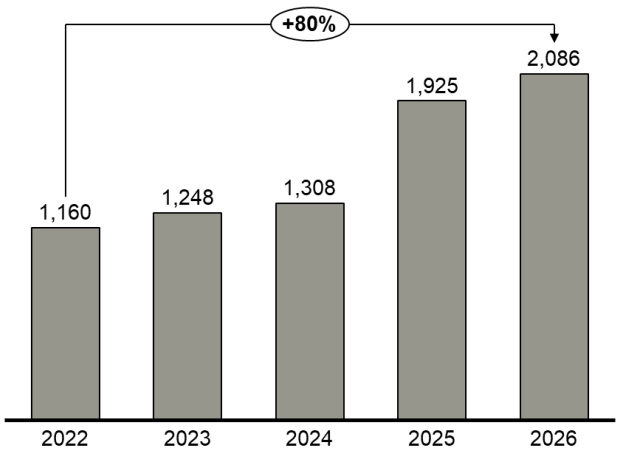
[19] Cybersecurity Risk Assessment: the evaluation of systems and processes to identify vulnerabilities and determine appropriate mitigation actions.

[20] Incident Response: the coordinated activities used to detect, analyze, contain, and remediate cybersecurity incidents.

B. Increasing Attacks on Energy Infrastructure

Globally and domestically, cybersecurity risk is steadily increasing. Year over year, from Q1 2025 to Q1 2026, the average weekly cyberattacks per global organization increased by 10%. In the four years since the Companies' last GRC filing, cyberattacks against global organizations are up 80%, as seen in Figure OZ-1.[21] The Office of Cybersecurity, Energy Security, and Emergency Response at the U.S. Department of Energy specifically recognizes this trend of persistent threats to critical energy infrastructure in the United States, and its potential severe and cascading effects, as part of its strategic plan for 2026 through 2030.[22]

FIGURE OZ-1
Global Average Weekly Cybersecurity Attacks per Organization in Q1[23]



At the Companies, cybersecurity is critical to the safe and reliable delivery of electric and gas services to customers, including critical infrastructure providers in the service territory (*e.g.*, financial services, telecommunication providers, other utilities). SoCalGas's and SDG&E's service territories include millions of people, one of the nation's busiest ports, some of the largest cities in California, critical military bases, defense contractors, and small businesses. In

---

[21] Check Point, *Global Cyber Attacks Remain Near Record Highs in February 2026 Despite Ransomware Decline* (March 10, 2026), *available at*: https://blog.checkpoint.com/research/global-cyber-attacks-remain-near-record-highs-in-february-2026-despite-ransomware-decline/.

[22] U.S. Department of Energy – Office of Cybersecurity, Energy Security, and Emergency Response (CESER), *CESER Strategic Plan, Fiscal Years 2026–2030* (March 2026), *available at:* https://www.energy.gov/documents/ceser-strategic-plan2026-2030.

[23] *Id.*

2028, the Companies' service territories will be subject to heightened global visibility associated with the hosting of a major international event in Los Angeles. Periods of increased visibility and critical-infrastructure reliance are commonly considered in cybersecurity risk planning due to the potential for elevated threat interest.[24] Critical utility infrastructure, such as that owned and maintained by the Companies, will remain a high-value, high-impact cyberattack target. Combined, these factors continue to create an elevated cybersecurity risk environment.

Unlike other utility risks, cybersecurity events may be deliberately caused by intelligent, adaptive adversaries seeking to achieve criminal, financial, or disruptive objectives, or may arise from non-malicious conditions such as system or application misconfigurations, limitations in patch availability, or vulnerabilities for which no security patch yet exists. Similarly, the risk events are caused by actors that actively observe defensive measures, exploit human and technical weaknesses, and adjust their methods to bypass controls. Because of this, Cybersecurity risk cannot be managed solely through traditional, condition-based, or reactive risk mitigation approaches. Instead, cybersecurity requires a proactive continuously evolving program focused on prevention, real-time detection, rapid response, and resilience to reduce the likelihood and potential impact of deliberate cybersecurity events on system reliability, safety, and customer service. Cybersecurity threats have continued to evolve, increase, and become more complex and impactful year over year, as adversaries continue to use an evolving and increasingly sophisticated set of tools and strategies to conduct attacks on the energy sector. Their suite of capabilities has historically included advanced malware,[25] complex phishing attacks, identification of non-public vulnerabilities, and ransomware,[26] but is evolving to include more sophisticated attacks enabled by advancements in artificial intelligence (AI) and quantum computing, including deepfakes and decryption. Industry reporting indicates that adversaries are increasingly leveraging AI to automate reconnaissance, accelerate vulnerability discovery, scale social engineering campaigns, and generate more convincing impersonation and disinformation

---

[24] Los Angeles Department of Water and Power (LADWP), *Sixth Annual Utility Trends Briefing on Preparation for the 2028 Olympic Games: Legislative and Program Updates* (January 9, 2024), *available at*: https://ladwpnews.com/ladwps-sixth-annual-utility-trends-briefing-on-preparation-for-the-2028-olympic-games-legislative-and-program-updates/.

[25] Malware: malicious software used to disrupt systems, gain unauthorized access, or damage data.

[26] Ransomware: malicious software that restricts access to systems or data and demands payment for restoration.

content. Separately, industry reporting also describes defensive initiatives using advanced AI to identify previously undiscovered software vulnerabilities in widely deployed technologies (e.g., Anthropic's Project Glasswing),[27] underscoring that AI can accelerate vulnerability discovery beyond traditional methods.

Further, as the volume of distributed energy resources increases, the need for organizations to expand operational technology (OT) visibility and cybersecurity monitoring capabilities also increases, as they contribute to a larger attack surface which can complicate detection, root cause analysis, and response to cyberattacks on the energy system.[28]

C. Adversarial Nation-States and Criminal Actors Continue to Pose Immense Cyber Risk

Cyberattacks on energy infrastructure are not hypothetical and have occurred both domestically and internationally. For example, recent U.S. cyber incidents affecting critical infrastructure operators, including American Water[29] and the Littleton Electric Light & Water Department[30], illustrate how malicious actors can disrupt operational environments and degrade visibility and control when technology is exposed or insufficiently protected.

As another recent example, in December 2025, a malicious cyberattack compromised the operational technology and industrial control systems[31] in Poland's energy sector. The bad actors gained access through vulnerable internet-facing edge devices causing loss of view and control between facilities and distribution system operators. Threats of this nature remain a significant concern for energy-sector environments, where outdated hardware can provide an initial access point into control networks. The Poland incident demonstrates that once adversaries

---

[27] Anthropic, *Project Glasswing: Securing critical software for the AI era*, *available at*: https://www.anthropic.com/glasswing.

[28] Dragos, *2026 OT Cybersecurity Year in Review* (February 2026) at 62-91, *available at:* https://www.dragos.com/ot-cybersecurity-year-in-review.

[29] TechTarget, *The American Water Cyberattack: Explaining How It Happened* (October 18, 2024), *available at:* https://www.techtarget.com/whatis/feature/The-American-Water-cyberattack-Explaining-how-it-happened.

[30] Industrial Cyber, *Dragos Details LELWD's Fight Against VOLTZITE Cyberattack, Following 300-Day OT Network Breach* (March 13, 2025), *available at:* https://industrialcyber.co/utilities-energy-power-water-waste/dragos-details-lelwds-fight-against-voltzite-cyberattack-following-300-day-ot-network-breach/.

[31] Industrial Control Systems: integrated hardware and software systems used to monitor, control, and automate industrial processes across sectors like manufacturing, energy, and water treatment.

compromise these devices, they can disrupt operator visibility, corrupt firmware, and degrade control functions. These vulnerabilities pose substantial risks to operational continuity and overall energy system reliability.[32]

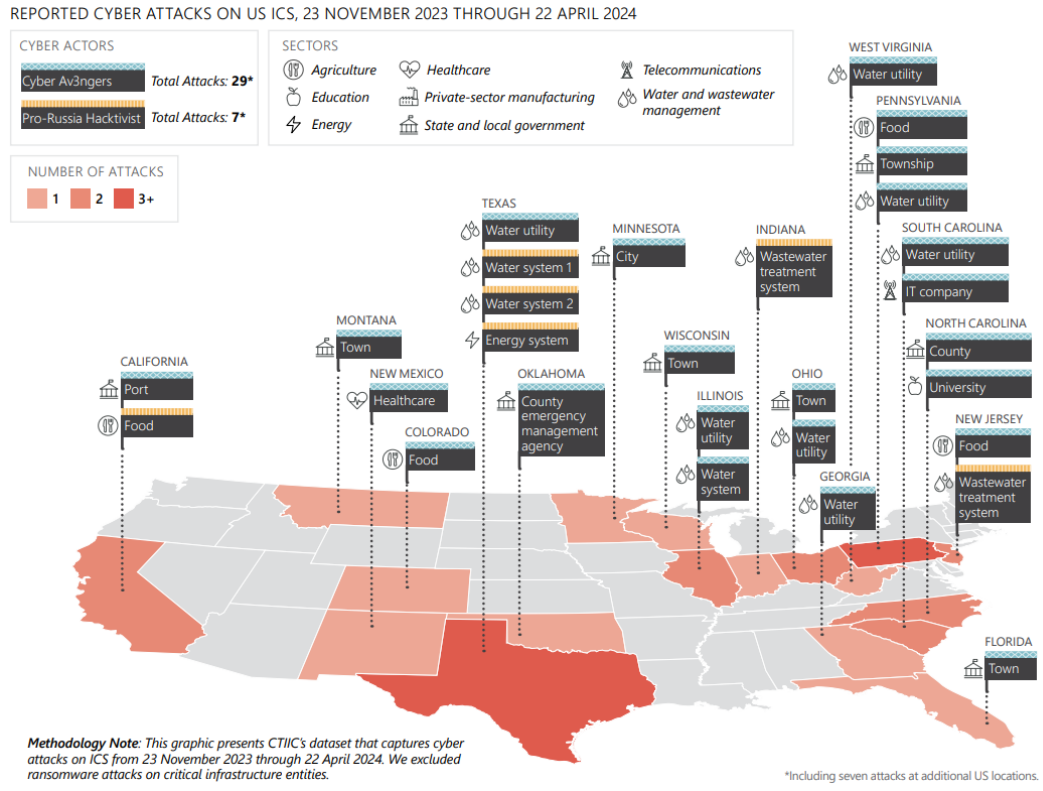
The criticality of cybersecurity is heightened by the breadth of adversaries the Companies face. These adversaries include diverse types of actors with varying intent to cause harm; they are not just criminal entities or hackers looking to make a political statement or achieve financial gain, but also include advanced adversaries, often aligned to nation-states, which are targeting critical infrastructure for economic exploitation, espionage, or covert action in preparation for some overt act (*e.g.*, disrupting energy supply). For example, in just a five-month period between 2023-2024, nation-state cyber actors affiliated with Iran and Russia attacked U.S. industrial control systems (ICS) at least 36 times, demonstrating the ability for adversaries to compromise operational technology, like that deployed by SoCalGas and SDG&E, and the necessity to invest in defenses to protect against such adversarial attacks.[33] Figure OZ-2 below shows the breadth of ICS cyberattacks over a 6 month period targeting utilities and their respective infrastructure in the US.

[32] Cybersecurity and Infrastructure Security Agency (CISA), *Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps* (February 10, 2026), *available at*: https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps.

[33] Office of the Director of National Intelligence, *Recent Cyber Attacks on U.S. Infrastructure Underscore Vulnerability of Critical U.S. Systems, November 2023–April 2024* (June 2024), *available at*: https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf.

FIGURE OZ-2

Domestic Cyberattacks in United States between November 2023 and April 2024



In this broader threat environment, the volume and persistence of cyber activity utilities are facing continues to grow significantly. Industry reporting indicates that in 2025, 53 percent of OT security assessments identified findings related to Internet-connected or externally exposed assets, with the electric sector representing 19 percent of those exposure findings. Over 50 percent of those findings were classified as critical or high severity.[34] This data underscores the operational risk associated with externally facing infrastructure in the utility environment. Internally, over the past year, the Companies have blocked an average of 10 million potentially malicious emails and remediated 140,000+ vulnerabilities each month. Perimeter Defenses[35] have further blocked over 14 million application activity instances.[36] Figures OZ-3 and OZ-4

[34] Dragos, *2026 OT Cybersecurity Year in Review* (February 2026) at 15, *available at:* https://www.dragos.com/ot-cybersecurity-year-in-review.

[35] Perimeter Defenses: Controls that monitor and protect external access points to systems and networks.

[36] SDG&E Cybersecurity System Operations (SysOps) Reporting (January 5, 2025)

below demonstrate the immense and consistent volume of attack attempts that have been blocked by the Companies' cybersecurity defenses:

FIGURE OZ-3

Highest Volume Connection Threats Blocked, 2025

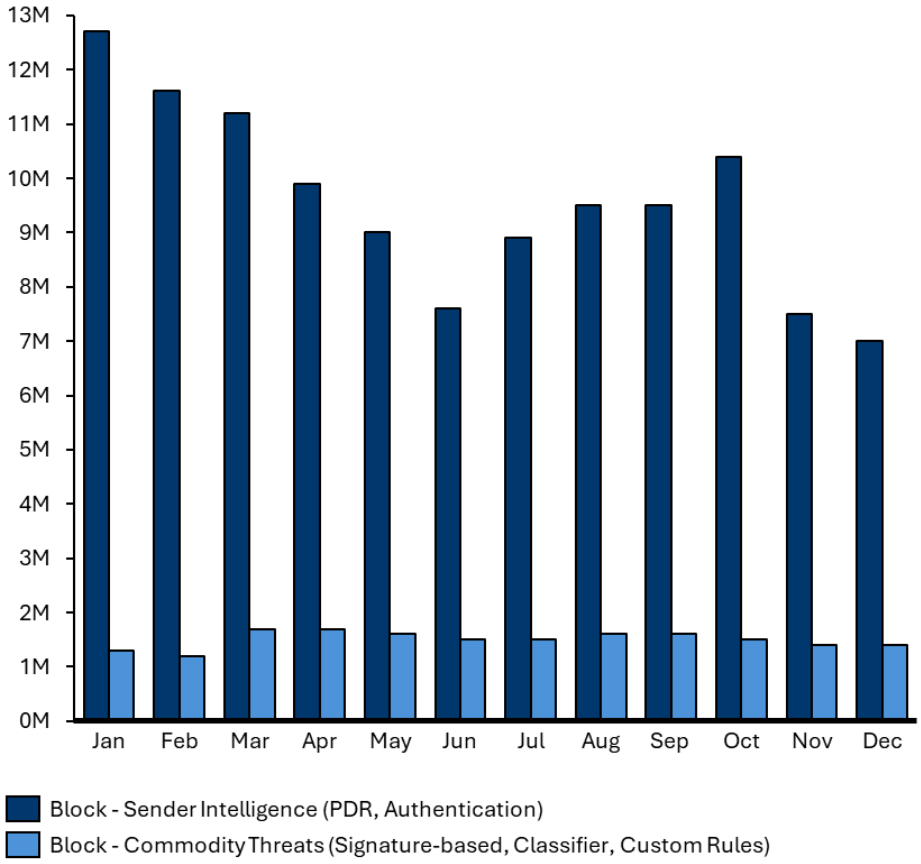
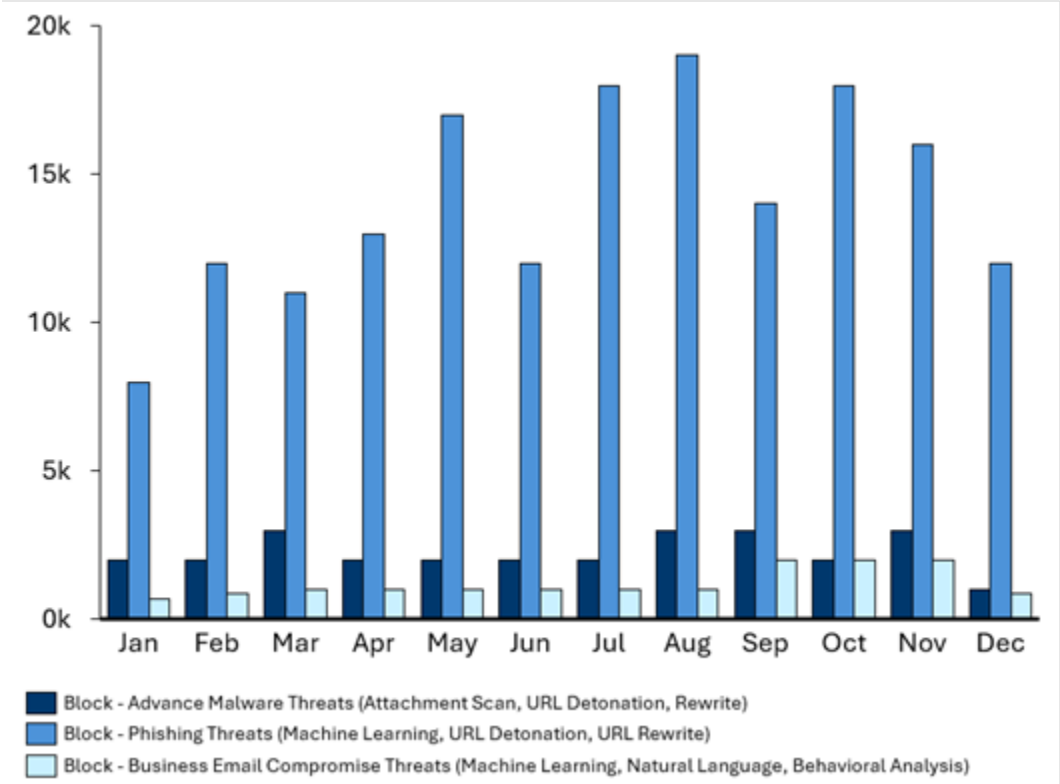


FIGURE OZ-4
Additional Connection Threats Blocked, 2025



Over the last 5 years, cybersecurity attacks and breaches have continued to target electric and gas utilities in the United States. Some examples of attacks which have breached perimeter defenses, interior defenses, and allowed unauthorized access to critical infrastructure include:

- Colonial Pipeline Group: On May 8, 2021, a criminal-network ransomware attack triggered one of the largest operators of fuel pipelines in the United States to shut down its operations to prevent the bad actor from migrating from its IT systems to its OT systems.[37] The attack disrupted nearly half of the fuel supply for the East Coast and disrupted energy markets and the supply of gas and diesel from the Gulf of Mexico to the East Coast.

[37] TechTarget, *Colonial Pipeline hack explained: Everything you need to know* (April 26, 2022), *available at:* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know; *see also* BBC News, *Colonial hack: How did cyber-attackers shut off pipeline?* (May 10, 2021), *available at:* https://www.bbc.com/news/technology-57063636.

- Lazarus Group: In 2022, security researchers reported that the North Korea-linked Lazarus Group carried out a cyber intrusion against the business IT networks of multiple energy companies in the US, Canada, and Japan. It also gained unauthorized access through a known software flaw and deploying tools to maintain ongoing access. The incident required investigation and remediation efforts to limit potential exposure of sensitive systems and information.[38]

- Duke Energy Florida and American Electric Power: In 2025, a threat actor claimed to have obtained and offered approximately 139 gigabytes of engineering and detailed infrastructure mapping data for sale after hacking a third-party vendor that provides services to Duke Energy Florida and American Electric Power. This incident demonstrated the vulnerabilities from vendor partners in the utilities supply chain. The utility involved was unable to grasp the full scope or cause of the attack for months, potentially leaving the vulnerability for potential exploitation in the future.[39]

These factors underscore the critical need for robust threat identification, proactive risk mitigation, and lifecycle vulnerability management (from discovery to remediation) to reduce the likelihood of exploitation of sensitive systems and strengthen the Companies' overall resilience.

Risks associated with supply chain and unauthorized disclosure of sensitive information also continue to increase[40]. Recent examples include the 2023 cybersecurity breach affecting a gas-sector operator, Suncor Energy's Petro-Canada subsidiary,[41] which disrupted customer payment systems and exposed customer information, and the 2024 ransomware and data-theft

---

[38] Cybersecurity Dive, *Energy providers hit by North Korea-linked Lazarus exploiting Log4j VMware vulnerabilities* (September 13, 2022), *available at*: https://www.cybersecuritydive.com/news/energy-providers-log4j-vmware/631673/.

[39] IT Pro, *Hacker offering US engineering firm data online after alleged breach* (January 7, 2026), *available at*: https://www.itpro.com/security/cyber-attacks/hacker-offering-us-engineering-firm-data-online-after-alleged-breach.

[40] Industrial Cyber, *Pickett USA Breach Allegedly Exposes Sensitive Engineering Data Linked to U.S. Utilities* (January 2026), *available at:* https://industrialcyber.co/utilities-energy-power-water-waste/pickett-usa-breach-allegedly-exposes-sensitive-engineering-data-linked-to-us-utilities/.

[41] Cybersecurity Dive, *Suncor Hackers Breached Petro-Canada Customer Data* (July 6, 2023), *available at*: https://www.cybersecuritydive.com/news/suncor-hackers-breached-petro-canada-customer-data/685365/.

incidents affecting Schneider Electric's platforms supporting electric and energy-sector operations.[42] Collectively, these examples demonstrate that cybersecurity risks to utilities arise from multiple threat vectors, reinforcing the need for layered, continuously maturing controls to protect electric and gas system operations and sensitive information. The Companies' cybersecurity mitigation activities apply lessons learned from these threats and other events, assessments, and exercises to identify and deploy cybersecurity improvements designed to protect sensitive information and enterprise systems. Note per IBM's Cost of a Data Breach Report, the 'average [cost of a data breach in] …the United States, …surged by 9% to USD 10.22 million, an all-time high for any region. Higher regulatory fines and higher detection and escalation costs in the United States contributed to this surge.'

In addition to the persistent and increasing volume of traditional cyber threats, the Companies are facing a new class of emerging threats that materially change the nature of cybersecurity risk. These threats are characterized by rapid evolution, increased automation, and the use of advanced technologies that can amplify both the scale and effectiveness of cyberattacks. Artificial intelligence is a key driver of this shift and represents one of several emerging threat vectors that the Companies must proactively address.

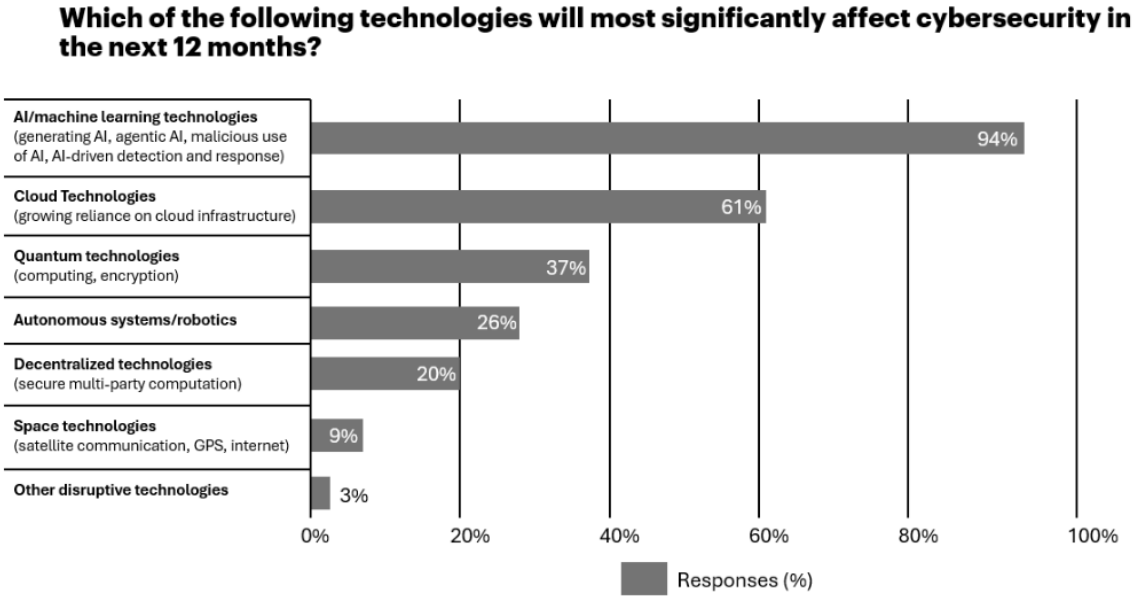
AI is fundamentally reshaping the cybersecurity landscape by simultaneously increasing risk and improving defensive capability. Figure OZ-5 below shows results from the World Economic Forum's 2026 Global Cybersecurity Outlook in which 94% of respondents named AI and machine learning technologies as the category of technology that will be most likely to impact organizations' cybersecurity.[43]

---

[42] Bleeping Computer, *Schneider Electric Confirms Dev Platform Breach After Hacker Steals Data*, (November 4, 2024), *available at*: https://www.bleepingcomputer.com/news/security/schneider-electric-confirms-dev-platform-breach-after-hacker-steals-data/.

[43] World Economic Forum, *Global Cybersecurity Outlook 2026* (January 2026), *available at*: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.

FIGURE OZ-5
Cybersecurity Professionals Outlook on Technology Impacts in 2026



D. Role of Artificial Intelligence

Artificial intelligence impacts organizations by expanding the attack surface. First, AI empowers external threat actors. Adversaries are now using AI to automate reconnaissance, scale attacks, evade detection, exploit vulnerabilities more rapidly, and generate sophisticated malware and social-engineering campaigns, including deepfake content that can undermine trusted business processes. Public reporting on Anthropic's "Project Glasswing" describes the use of advanced AI models in a controlled setting to identify previously unknown software vulnerabilities in widely deployed systems, underscoring that AI can accelerate the discovery of latent vulnerabilities in vendor-provided technologies.[44]

AI-enabled attacks are increasingly difficult to distinguish from legitimate activity, producing content and behaviors that are more convincing, context-aware, and harder for both users and traditional detection tools to identify as malicious. In addition, AI-based code generation tools enable threat actors to develop and modify malware more rapidly, increasing the volume, variation, and evasiveness of malicious software encountered by defenders. Recent cyber-intelligence reporting further corroborates this trend, demonstrating that single actors can

[44] Anthropic, *Project Glasswing: Securing critical software for the AI era*, *available at*: https://www.anthropic.com/glasswing.

now generate operationally mature malware frameworks in days using commercially available AI tooling.[45] AI also can increase the risks associated with insider threats: the rapid adoption of AI tools by employees and contractors and growing use of AI embedded within vendor products introduce new vectors for data exposure, model manipulation, supply chain compromise, and misuse of sensitive information.

However, AI is not only a tool that can be used by adversaries and threat actors to expose organizations to malicious activities. Organizations and their vendor partners are also increasingly embedding AI capabilities into threat detections and defenses. AI can enhance defense capabilities. When responsibly integrated into cyber defenses it can strengthen the Companies' ability to identify and mitigate threats earlier, reduce operational risk, and support more efficient and cost-effective cybersecurity operations for customers. As the AI environment continues to rapidly evolve, organizations must continue to adapt and be flexible, investing in not just AI tools, but in AI protections and controls.

E. Overall Cost Drivers

Cybersecurity is a shared service for SDG&E, SoCalGas, and Corporate Center,[46] and the costs set forth in my testimony are allocated between the Companies based on the mechanisms described in the Shared Services testimony (Ex. SCG-22/SDGE-27). The cybersecurity risk mitigation activities set forth in my testimony correspondingly benefit SDG&E, SoCalGas, and Corporate Center. The primary drivers for the cybersecurity costs discussed in this testimony are for the enhancement or addition of new technical capabilities to address evolving threats and accommodate innovative technologies implemented by other business units, replacement of unsupported systems and cybersecurity technology, and increasing costs to maintain and support existing cybersecurity technologies. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were moved to the Cybersecurity forecast to more accurately reflect their direct role in protecting

[45] Check Point Research, *Cybersecurity Report 2026* at 65 (Figure 5) (January 28, 2028), *available at:* https://research.checkpoint.com/2026/cyber-security-report-2026/.

[46] Cybersecurity is a shared service for both utilities except for Operational Technology systems, which are specific to each utility (*i.e.,* gas control infrastructure at SoCalGas and electric grid control infrastructure at SDG&E).

critical infrastructure, operational technology environments, and sensitive data, along with changes in the cybersecurity technology market.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost increases are entirely outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators. The Companies' cybersecurity forecast is prudent and reasonable to address the existing and growing cybersecurity threat and mitigate the risk of negative consequences for reliability, and customer and employee safety.

Some of the fundamental activities required to support and effectively manage cybersecurity capabilities include, but are not limited to, the following investments:

- Risk Mitigation
  - Support the implementation and ongoing operation of enterprise-wide cybersecurity policies, standards, and governance frameworks developed and managed by the Corporate Center, including utility-specific procedures and controls.
  - Evaluate, manage and monitor IT, Operational Technology (OT), and third-party cyber risks, including conducting periodic assessments
  - Vulnerability management, including the identification, prioritization, tracking, and remediation of vulnerabilities across IT, OT, and cloud environments.
  - Monitor compliance, identify vulnerabilities, and drive remediation activities
- Identity and Access Control
  - Design, implement, and manage access controls, including privileged access management
  - Operate and maintain system authentication services, including public key infrastructure (PKI)

- Protective Technologies
  - Design, implement, and maintain network, endpoint, user, and application security controls
  - Design, implement, and enforce data protection capabilities, including encryption, data loss prevention, and secure data handling
- Monitoring and Detection
  - Operate and enhance Security Operations Center (SOC) capabilities and the Insider Threat program to monitor security-related activities across users, systems, assets, and applications
  - Detect, analyze, correlate, and escalate anomalies and security events
- Response, Recovery, and Resilience
  - Develop, coordinate, and execute incident response plans
  - Plan, conduct, and evaluate cybersecurity exercises and drills to validate readiness and response effectiveness
- Architecture and Asset Visibility
  - Design, implement, and maintain cybersecurity architecture and segmentation, including OT network zoning and isolation
  - Scan assets for compliance with hardening standards and manage cybersecurity-related configurations for IT and OT systems to support visibility, monitoring, and incident response
  - Evaluate AI and AI-driven capabilities embedded in new and existing tools to identify cybersecurity risks introduced by these features, including assessing alignment with the Companies' AI security standards and applicable regulatory frameworks
  - Evaluate AI and AI-driven capabilities that can support the Companies Cybersecurity mitigation efforts

The details of my O&M and Capital requests can be found in sections III, IV, and VI below.

F. Organization of Testimony

My testimony is organized as follows:

- Section II discusses SDG&E's and SoCalGas's focus on affordability and efficiency.
- Section III provides the non-shared SDG&E and SoCalGas O&M costs.
- Section IV provides the shared O&M costs.
- Section V provides a summary of SDG&E and SoCalGas's RAMP O&M activities and a description of the selection and prioritization methodology for RAMP risk mitigations.
- Section VI presents the planned capital categories across SDG&E and SoCalGas.
- Section VII provides a summary of SDG&E and SoCalGas's RAMP Capital activities and a description of the selection and prioritization methodology for RAMP risk mitigations.
- Section VIII provides a summary of the risk controls and benefit cost ratios, justification for proposed mitigations with positive benefit cost ratios, changes from the 2025 RAMP Report.
- Section IX concludes with a recap of my requests.
- Section X sets forth my witness qualifications.

G. Support To and From Other Witnesses

My testimony also references the testimony and workpapers of other areas, either in support of their testimony or as referential support for mine. Those witness areas are Ex. SCG-10/SDGE-14, Information Technology, Ex. SCG-02/SDGE-02, Risk Philosophy, and Ex. SCG-22/SDGE-27, Shared Services.

II. AFFORDABILITY & EFFICIENCY

SDG&E and SoCalGas manage cybersecurity activities and costs using a risk-based approach that concentrates resources on reducing the likelihood and impact of the highest consequence cyber risks in the most cost-effective manner possible. Rather than attempting to address all threats equally, investments are prioritized based on risk, regulatory requirements, and potential impacts to safety and system reliability. This approach, implemented through the Companies' RAMP process, focuses spending on mitigations that deliver meaningful risk

mitigation while avoiding lower value or duplicative activities. By targeting resources where they are most effective, the Companies reduce the probability of disruptive cyber incidents that would result in significantly higher costs to customers from service interruptions, emergency response, and system recovery.[47] For further details on the chosen approach and alternative portfolios analysis, reference Chapter SCG-RISK-8/SDG&E-RISK-8, Cybersecurity.

Cybersecurity initiatives that support efficient defense against internal and external threats and cybersecurity vulnerabilities include threat intelligence[48] and cybersecurity training. The Companies' cybersecurity program emphasizes the use of threat intelligence to focus resources where they are most needed and balance Company-sourced cyber threat intelligence reporting with participation in federal, state, and industry information-sharing organizations, leveraging shared intelligence to inform defensive actions. This approach allows for efficiency in prioritizing threats and emerging trends to determine those which are most relevant to the Companies.

III. NON-SHARED O&M COSTS

"Non-Shared Services" are activities that are performed by a utility solely for its own benefit. Corporate Center provides certain services to the utilities and to other subsidiaries. For purposes of this general rate case, SoCalGas and SDG&E treat costs for services received from Corporate Center as Non-Shared Services costs, consistent with any other outside vendor costs incurred by the utilities. These activities include the routine operational workload needed to maintain the effectiveness of existing security controls and prevent degradation of the Companies' cybersecurity posture. Table OZ-2 summarizes the total non-shared O&M forecasts for SDG&E and Table OZ-3 summarizes the total non-shared O&M forecasts for SoCalGas by category of management.

---

[47] *See* A.25-05-010/013 (cons.), Volume 2, Chapter SCG-Risk-8/SDG&E-Risk-8, Cybersecurity for more information on the portfolio analysis and approach for cybersecurity.

[48] Threat Intelligence: information about threats and vulnerabilities used to inform cybersecurity defenses and mitigation strategies.

TABLE OZ-2
SDG&E Non-Shared O&M Summary of Costs

SDG&E CYBERSECURITY (In 2025 $)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Non-Shared Services	1,385	1,322	-63
Total Non-Shared Services	**1,385**	**1,322**	**-63**

TABLE OZ-3
SoCalGas Non-Shared O&M Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Non-Shared Services	2,398	2,343	-55
Total Non-Shared Services	**2,398**	**2,343**	**-55**

A. Non-Shared Cybersecurity O&M – SDG&E and SoCalGas

TABLE OZ-4
SDG&E Non-Shared O&M Summary of Costs by Workpaper in 2025 Dollars ($000s)

SDG&E CYBERSECURITY (In 2025 $)			
A. Cybersecurity	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
1. NON-SHARED PERIMETER DEFENSES	85	19	-66
2. NON-SHARED INTERNAL DEFENSES	1,245	1,245	0
3. NON-SHARED SENSITIVE DATA PROTECTION	55	58	3
Total	**1,385**	**1,322**	**-63**

TABLE OZ-5
SoCalGas Non-Shared O&M Summary of Costs by Workpaper in 2025 Dollars ($000s)

SCG CYBERSECURITY (In 2025 $)			
A. Cybersecurity	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
1. NON-SHARED PERIMETER DEFENSES	112	2	-110
2. NON-SHARED INTERNAL DEFENSES	2,286	2,341	55
Total	**2,398**	**2,343**	**-55**

1. Forecast Method

The forecast methodology developed for this cost category is the base year (2025) recorded. This forecast methodology is appropriate because history is not always a good predictor of future needs for Cybersecurity. The pace of change in the cybersecurity industry continues to accelerate when compared to prior years. Costs for existing vendor contracts and services are increasing rapidly to sustain defense and effectiveness. An evolving threat landscape, cybersecurity attacker sophistication, and threat complexity requires the Companies to use current data and forecast adjustments rather than relying on historical averages that do not account for increased defenses needed to combat growing cybersecurity threats.

2. Perimeter Defenses

a. Description of Costs and Underlying Activities

Although these cybersecurity activities are functionally similar to shared services, they are classified as non-shared because they support systems, assets, and operational environments that are unique to the individual utility and are not performed on shared enterprise platforms. These non-shared SDG&E and SoCalGas cybersecurity costs represent the perimeter defenses portion of cybersecurity labor and non-labor O&M activities that are retained by the Companies and are not part of shared services. These activities are the day-to-day cybersecurity work the Companies undertake to prevent, detect, and respond to attempted cyber intrusions. In this category, non-shared SDG&E and SoCalGas cybersecurity costs include threat intelligence, security tool maintenance, compliance oversight, cloud security, audit remediation, and incident response retainer services. Together, these efforts represent the routine operational workload

required to maintain the effectiveness of existing security controls and prevent degradation of the Companies' cybersecurity posture.

These costs are reasonable and necessary to maintain secure and reliable utility operations and to support the Companies' risk-based controls and mitigations included in this GRC. Cybersecurity is a RAMP-designated workpaper and the non-shared O&M activities are required to support controls and mitigations that enable the safe and reliable delivery of electric and gas services to the Companies' customers. Information regarding Perimeter Defense is found in the non-shared O&M workpapers. Ex. SCG-11-WP (2CS001.000 / SDG&E-15-WP (1CS001.000).

b. Cost Drivers

The O&M forecast is driven by the continuing need to address the Companies' increasing exposure to cybersecurity risk affecting critical energy infrastructure and customer-serving systems. Threat activity targeting the energy and utilities sectors continues to escalate; in North America, organizations in this sector experienced a 112% year-over-year increase in average weekly cyberattacks between 2022 and 2026,[49] reflecting materially higher operational and systemic risk. As threat activity increases in volume, sophistication, and frequency, the Companies must sustain higher levels of ongoing monitoring, analysis, access management, tool maintenance, compliance oversight, and incident readiness, which directly increases the recurring operational workload required to maintain the effectiveness of existing perimeter defenses.

3. Internal Defenses

a. Description of Costs and Underlying Activities

Internal defense activities represent cybersecurity labor and non-labor efforts focused on securing internally managed systems, identities, and data environments that are not externally facing and not provided through shared or perimeter-based services. These activities are primarily workload-driven, ongoing in nature, and necessary to maintain core cybersecurity functions such as continuous monitoring, vulnerability remediation, identity and access

[49] Check Point, *Global Cyber Attacks Remain Near Record Highs in February 2026 Despite Ransomware Decline* (March 10, 2026), *available at*: https://blog.checkpoint.com/research/global-cyber-attacks-remain-near-record-highs-in-february-2026-despite-ransomware-decline/; *see also* Check Point, *Cybersecurity Report 2023*, *available at*: https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023.

governance, and incident response within the Companies' internal environments. Without funding for these activities, the Companies would be at greater risk to becoming a victim of a cyberattack.

These costs are reasonable and necessary to maintain secure and reliable utility operations and to support the Companies' risk-based controls and mitigations included in this GRC. Cybersecurity is a RAMP-designated workpaper and the non-shared O&M activities are required to support controls and mitigations that enable the safe and reliable delivery of electric and gas services to the Companies' customers. Information regarding Internal Defense is found in the non-shared O&M workpapers. Ex. SCG-11-WP (2CS002.000) / SDGE-15-WP (1CS002.000).

b. Cost Drivers

The O&M forecast is driven by the continuing need to address the Companies' increasing exposure to cybersecurity risk affecting critical energy infrastructure and customer-serving systems. Threat activity targeting the energy and utilities sector continues to escalate; in North America, organizations in this sector experienced a 112% year-over-year increase in average weekly cyberattacks between 2022 and 2026[50] reflecting materially higher operational and systemic risk. Increased exposure directly translates into higher cybersecurity operating costs because it requires additional analyst and engineering time to review and triage a greater volume of potential cyber events, analyze expanded threat intelligence, continuously tune cybersecurity tools to address more sophisticated threats, and manage an increased volume of vulnerabilities and system hardening activities.

4. Sensitive Data Protections

a. Description of Costs and Underlying Activities

Although these cybersecurity activities are functionally similar to shared services, they are classified as non-shared because they support systems, assets, and operational environments that are unique to the individual utility and are not performed on shared enterprise platforms.

---

[50] Check Point, *Global Cyber Attacks Remain Near Record Highs in February 2026 Despite Ransomware Decline* (March 10, 2026), *available at*: https://blog.checkpoint.com/research/global-cyber-attacks-remain-near-record-highs-in-february-2026-despite-ransomware-decline/; *see also* Check Point, *Cybersecurity Report 2023*, *available at*: https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023.

These non-shared SDG&E cybersecurity costs represent the sensitive data protections[51] portion of cybersecurity labor and nonlabor activities that are retained by the Company and are not part of shared services. These activities encompass the work required to protect the Companies' systems, infrastructure, and operational technologies. To effectively mitigate risk, ongoing O&M funding is necessary to maintain core cybersecurity functions, including vulnerability management,[52] identity and access governance, security tool maintenance, compliance oversight, cloud security, audit remediation, and incident response retainer services. Together, these efforts represent the routine operational workload needed to maintain the effectiveness of existing security controls and prevent degradation of the Companies' cybersecurity posture. Without funding for these activities, the Companies would be at greater risk to becoming a victim of a cyberattack.

These costs are reasonable and necessary to maintain secure and reliable utility operations and to support the Company's risk-based controls and mitigations included in this GRC. Cybersecurity is a RAMP-designated workpaper and the non-shared O&M activities are required to support controls and mitigations that enable the safe and reliable delivery of electric and gas services to the Company's customers. SoCalGas does not support any non-shared sensitive data protections cybersecurity costs. Information regarding Sensitive Data Protection is found in the non-shared O&M workpaper. Ex. SDGE-15-WP (1CS003.000).

b. Cost Drivers

The O&M forecast is driven by the continuing need to address the Company's increasing exposure to cybersecurity risk affecting critical energy infrastructure and customer serving systems. Threat activity targeting the energy and utilities sector continues to escalate; in North America, organizations in this sector experienced a 112% increase in average weekly cyberattacks between 2022 and 2026[53] reflecting materially higher operational and systemic

---

[51] Sensitive Data Protections: Controls and processes used to safeguard customer, employee, and company information from unauthorized access or disclosure.

[52] Vulnerability Management: the process of identifying, evaluating, and remediating system weaknesses to reduce cybersecurity risk.

[53] Check Point, *Global Cyber Attacks Remain Near Record Highs in February 2026 Despite Ransomware Decline* (March 10, 2026), *available at*: https://blog.checkpoint.com/research/global-cyber-attacks-remain-near-record-highs-in-february-2026-despite-ransomware-decline/; *see also* Check Point, *Cybersecurity Report 2023*, *available at*: https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023.

risk. As discussed above in section III.2.b, this increased exposure results in higher cybersecurity operating costs by driving additional analyst and engineering effort to monitor, analyze, tune, and remediate against a larger and more sophisticated volume of cyber threats.

IV. SHARED O&M COSTS

Shared Services are activities performed by a utility shared services department (*e.g.*, functional area) for the benefit of: (i) SDG&E or SoCalGas, (ii) Sempra Energy Corporate Center, and/or (iii) any affiliate subsidiaries. The utility providing Shared Services allocates and bills incurred costs to the entity or entities receiving those services. For Cybersecurity, Table OZ-4 summarizes the total shared O&M forecasts for the listed cost categories.

TABLE OZ-6
SDG&E Shared O&M Summary of Costs

SDG&E CYBERSECURITY (In 2025 $)			
(In 2025 $) Incurred Costs (100% Level)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Shared Services (Incurred)	10,566	12,396	1,830
Total Shared Services (Incurred)	**10,566**	**12,396**	**1,830**

TABLE OZ-7
SoCalGas Shared O&M Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)			
(In 2025 $) Incurred Costs (100% Level)			
Categories of Management	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
Total Shared Services	4,200	6,493	2,293
Total Shared Services (Incurred)	**4,200**	**6,493**	**2,293**

Forecasts are presented on a total incurred basis, as well as the shared services allocation percentages related to those costs. Those percentages are presented in my shared services workpapers, along with a description explaining the activities being allocated. *See* Ex. SCG-11-WP/SDGE-15-WP.

A. Shared Cybersecurity – SDG&E and SoCalGas

The shared Cybersecurity costs represent labor and non-labor for the Cybersecurity area where costs are shared among multiple business units and support the Companies' goals of safety, reliability, and resilience. The Cybersecurity O&M forecasts include the resources and systems maintenance needs for the functional groups described below:

B. Cybersecurity Functional Groups

The Cybersecurity organization includes several functional groups that collectively support the Companies' risk mitigation, operational defense, compliance, engineering assurance, workforce cybersecurity readiness, and secure enablement of business and technology initiatives. Together, these functions perform the governance, execution, advisory, and support activities necessary to operate a risk-based cybersecurity program. Each group has defined responsibilities that align to the Companies' cybersecurity controls, regulatory requirements, and mitigation activities described in this testimony. These functional groups are descriptive constructs used to organize cybersecurity activities and responsibilities; they do not represent discrete organizational units or separately funded cost centers.

C. Cybersecurity *Strategy, Portfolio and Governance*

The Cybersecurity Strategy, Portfolio and Governance function design, implement, and operate the controls to meet the requirements outlined by the corporate cybersecurity department and align cybersecurity initiatives with enterprise priorities. Responsibilities include document controls to support policies; implement controls and evaluation of operating effectiveness as required; manage any control findings and monitor remediation; and provides portfolio management, prioritization, coordination, and delivery oversight for cybersecurity initiatives. This function helps ensure that resources are directed to the highest-value, risk-mitigating activities and that new cybersecurity capabilities are deployed in a controlled and timely manner.

D. Cybersecurity *Threat Detection & Response*

Cybersecurity Threat Detection & Response encompasses the Security Operations Center (SOC) and related threat monitoring, detection, and response activities, including incident response, threat intelligence, and vulnerability management. These groups conduct 24/7 monitoring, alerting, analysis, incident handling, intelligence-driven defense, and proactive threat hunting. Collectively, they identify, analyze, contain, and mitigate cybersecurity incidents and suspicious activity to reduce operational and safety risk to the Companies.

E. Cybersecurity *Operations & Compliance*

The Cybersecurity Operations & Compliance function supports compliance with cybersecurity-related laws, rules, regulations, and internal control requirements. Responsibilities include coordinating cybersecurity and IT control assessments, managing evidence collection, validating required controls, and tracking remediation activities. This function provides compliance assurance and operational coordination that complements the Companies' defense and engineering groups.

F. Cybersecurity *Architecture & Engineering*

The Cybersecurity Architecture & Engineering function provides cybersecurity expertise and advisory support for business initiatives and technology projects. This function performs security assessments of systems, applications, and architectures, and evaluates cybersecurity controls used by vendors and third-party service providers. Cybersecurity Architecture & Engineering acts as an assurance capacity to help confirm that cybersecurity requirements are incorporated into business and technology designs prior to deployment.

G. Enterprise *Identity Services*

Manage identity lifecycle, authentication, and access controls across IT and OT environments to reduce the risk of unauthorized access and credential misuse.

H. Insider *Trust and Forensics*

Detect, investigate, and support response to potential insider threats, anomalous user activity, and cybersecurity incidents through forensic analysis and investigative support.

All cybersecurity-related activities and associated costs described in this section are sponsored and included in the forecast in my testimony.

TABLE OZ-8
SDG&E Shared O&M Summary of Costs by Workpaper
In 2025 Dollars ($000s)

SDG&E CYBERSECURITY (In 2025 $)			
(In 2025 $) Incurred Costs (100% Level)			
A. Cybersecurity	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
1. SHARED PERIMETER DEFENSES	2,980	1,870	-1,110
2. SHARED INTERNAL DEFENSES	7,062	9,977	2,915
3. SHARED SENSITIVE DATA PROTECTION	524	549	25
Incurred Costs Total	**10,566**	**12,396**	**1,830**

Table OZ-9
SoCalGas Shared O&M Summary of Costs by Workpaper
In 2025 Dollars ($000s)

SoCalGas CYBERSECURITY (In 2025 $)			
A. Cybersecurity	**2025 Adjusted-Recorded (000s)**	**TY2028 Est. (000s)**	**Change (000s)**
1. SHARED PERIMETER DEFENSES	1,475	767	-708
2. SHARED INTERNAL DEFENSES	2,725	5,726	3,001
Incurred Costs Total	**4,200**	**6,493**	**2,293**

1. Forecast Method

The forecast methodology developed for this cost category is the base year (2025) recorded. This forecast methodology is appropriate because history is not always a good predictor of future needs for Cybersecurity. The pace of change in the cybersecurity industry

continues to accelerate when compared to prior years. Costs for existing vendor contracts and services are increasing rapidly to sustain effective defenses. An evolving threat landscape, cybersecurity attack sophistication, and technological advancements require the use of current data as the forecast baseline, rather than relying on historical averages that do not account for increased investment needed to combat these growing cybersecurity threats.

2. Perimeter Defenses

a. Description of Costs and Underlying Activities

The shared Perimeter Defenses O&M costs support the ongoing operation and management of technologies that monitor, control, and protect external access to the Companies' IT and operational technology environments. Examples of Perimeter Defenses activities include:

- Continuous monitoring of external-facing security technologies that control and protect access to the Companies' IT and OT environments.
- Alert triage, investigation, insider-threat detection, and coordination of response actions for suspected perimeter intrusions or malicious activity at the network edge.
- Tuning and maintaining perimeter detection rules and policies to keep pace with evolving threats and reduce false positives.

As threat activity becomes more frequent and complex, these functions require sustained operational effort to maintain effective perimeter protection. Information regarding Perimeter Defense is found in the O&M workpapers, Ex. SCG-11-WP (2200-2491.000)/SDGE-15-WP (2100-3763.000)

b. Cost Drivers

As discussed above, the Companies have observed a similar upward trend of threat activity and increased operational and systemic risk. While automated tools support detection and prioritization, the growth in sophisticated and multi-vector[54] threats requires sustained human involvement for analysis, investigation, coordination, and response, making labor a key driver of cybersecurity O&M costs.

The increase in cybersecurity O&M is driven by measurable growth in required workload, not by generalized threat statistics. While overall attack volume has increased, the

[54] Multi-vector threats: Coordinated attacks using various methods to exploit vulnerabilities.

primary cost drivers are (1) a higher number of actionable vulnerabilities and alerts requiring complex analysis, (2) greater effort per case due to increased attack sophistication and multisystem impacts, and (3) expanded mandatory regulatory and compliance requirements that impose fixed, recurring work independent of attack volume. Each vulnerability, alert, and compliance obligation requires significant levels of labor for assessment, documentation, coordination, and remediation. These activities scale with system size, data volume, and regulatory scope, and cannot be fully automated. In addition, incremental O&M is required to operate and sustain prior cybersecurity capital investments; without corresponding O&M growth, the effectiveness of those investments would degrade.

Additionally, adhering to new and existing Federal and State privacy regulations has increased the Companies' cybersecurity program needs. For example, regulations adopted in 2025 by the California Privacy Protection Agency under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, require covered entities to conduct formal cybersecurity risk assessments and prepare for independent cybersecurity audits focused on the protection of personal and sensitive customer information (*see* Appendix C, Controls and Mitigations Compliance Driver Roadmap). These requirements, which are implemented through the Companies' Office of Customer Privacy, necessitate enhanced documentation, control validation, and ongoing assessment of cybersecurity practices. Accordingly, the requested increase reflects the minimum resources required to process a demonstrably larger and more complex cybersecurity workload, meet regulatory mandates identified in Appendix C, and sustain existing cybersecurity capabilities, rather than a discretionary expansion of scope.

3. Internal Defenses

a. Description of Costs and Underlying Activities

The shared SDG&E and SoCalGas Internal Defenses cybersecurity costs support the ongoing operation and management of controls designed to detect, prevent, and contain malicious activity within the Companies' environments after an initial access attempt has occurred. These activities focus on limiting lateral movement, preventing misuse of credentials, identifying anomalous behavior, and rapidly responding to threats that bypass perimeter controls.

Examples of Internal Defenses activities include:

- Continuous monitoring and alert triage focused on activity inside the Companies' environments after an initial access attempt.
- Incident response coordination and investigation of internal events, including efforts to identify and contain lateral movement and misuse of credentials.
- Vulnerability identification and remediation, and risk-based assessment and compliance activities performed on shared enterprise platforms.

Because these defenses protect shared enterprise platforms and interconnected IT and operational technology environments, the associated labor and non-labor costs are performed centrally and allocated as shared services. Information regarding Internal Defense is found in the capital workpapers, Ex. SCG-11-CWP (2200-0944.000)/SDGE-15-CWP (2100-3101.000).

b. Cost Drivers

As discussed above, the Companies have observed a similar upward trend of threat activity and increased operational and systemic risk. As the volume of cybersecurity threats rises in parallel with them becoming more advanced and diverse, humans must remain part of the Companies' defenses.

The increase in cybersecurity O&M is driven by measurable growth in required workload, not by generalized threat statistics. While overall attack volume has increased, the primary cost drivers are (1) a higher number of actionable vulnerabilities and alerts requiring human analysis, (2) greater effort per case due to increased attack sophistication and multi-system impacts, and (3) new mandatory regulatory requirements that impose fixed, recurring work independent of attack counts. Each vulnerability, alert, and compliance obligation requires defined levels of labor for assessment, documentation, coordination, and remediation. These activities scale with system size, data volume, and regulatory scope and cannot be fully automated. In addition, incremental O&M is required to operate and sustain prior cybersecurity capital investments; without corresponding O&M growth, the effectiveness of those investments would degrade.

Additionally, adhering to new and existing Federal and State privacy regulations has increased the Companies' cybersecurity program needs. For example, regulations adopted in 2025 by the California Privacy Protection Agency under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, require covered entities to conduct formal

cybersecurity risk assessments and prepare for independent cybersecurity audits focused on the protection of personal and sensitive customer information.[55] These requirements, which are implemented through the Companies' Office of Customer Privacy, necessitate enhanced documentation, control validation, and ongoing assessment of cybersecurity practices. Accordingly, the requested increase reflects the minimum resources required to process a demonstrably larger and more complex cybersecurity workload, meet new regulatory mandates, and sustain existing cybersecurity capabilities, rather than a discretionary expansion of scope.

4. Sensitive Data Protection

a. Description of Costs and Underlying Activities

The shared SDG&E and SoCalGas Sensitive Data Protection cybersecurity costs support the ongoing operation and management of controls that protect sensitive customer, employee, and Company information from unauthorized access, disclosure, or misuse. Examples of Sensitive Data Protection activities include:

- Discovering and classifying sensitive customer, employee, and Company information across shared systems.
- Enforcing access controls, data loss prevention, and encryption to prevent unauthorized access, use, or disclosure of sensitive data.
- Monitoring movement of sensitive data and coordinating incident response activities related to potential data exposure events.

Because sensitive data is processed across shared enterprise platforms and business systems, these activities are performed centrally and allocated as shared services. The associated costs are driven by increasing data volumes, expanding regulatory privacy requirements, and the sustained operational effort required to monitor, validate, and maintain effective data protection controls. Information regarding Sensitive Data Protection is found in the capital workpapers, Ex. SDGE-15-CWP (2100-4128.000).

[55] *See, e.g.*, California Consumer Privacy Act (CCPA); Sarbanes-Oxley Act (SOX); CPUC Affiliate Transaction Compliance and other CPUC privacy decisions; California breach notification laws (Cal. Civ. Code §§ 1798.81.5, 1798.82); and Identity Theft Prevention (Federal Trade Commission (FTC) "Red Flags Rule"), among others.

b. Cost Drivers

As discussed above, the Companies have observed a similar upward trend of threat activity and increased operational and systemic risk. The Companies have similarly seen a directional increase in cyberattacks year-over-year. As the volume of cybersecurity threats rises while, in parallel, becoming more advanced and diverse, humans must remain in the loop as part of the Companies' defenses.

The increase in cybersecurity O&M is driven by measurable growth in required workload, not by generalized threat statistics. While overall attack volume has increased, the primary cost drivers are (1) a higher number of actionable vulnerabilities and alerts requiring human analysis, (2) greater effort per case due to increased attack sophistication and multi-system impacts, and (3) new mandatory regulatory requirements that impose fixed, recurring work independent of attack counts. Each vulnerability, alert, and compliance obligation requires defined levels of labor for assessment, documentation, coordination, and remediation. These activities scale with system size, data volume, and regulatory scope and cannot be fully automated. In addition, incremental O&M is required to operate and sustain prior cybersecurity capital investments; without corresponding O&M growth, the effectiveness of those investments would degrade.

Additionally, adhering to new and existing Federal and State privacy regulations has increased the Companies' cybersecurity program needs. For example, regulations adopted in 2025 by the California Privacy Protection Agency under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, require covered entities to conduct formal cybersecurity risk assessments and prepare for independent cybersecurity audits focused on the protection of personal and sensitive customer information.[56] These requirements, which are implemented through the Companies' Office of Customer Privacy, necessitate enhanced documentation, control validation, and ongoing assessment of cybersecurity practices. Accordingly, the requested increase reflects the minimum resources required to process a

[56] *See, e.g.*, CCPA; SOX; CPUC Affiliate Transaction Compliance and other CPUC privacy decisions; California breach notification laws (Cal. Civ. Code §§ 1798.81.5, 1798.82); and Identity Theft Prevention (FTC "Red Flags Rule"), among others.

demonstrably larger and more complex cybersecurity workload, meet new regulatory mandates, and sustain existing cybersecurity capabilities, rather than a discretionary expansion of scope.

V. RAMP INTO GRC – O&M

A. Description of RAMP Mitigations

The O&M activities described above in Sections III and IV were also presented in the 2025 RAMP Report and are listed in the tables below. Activities that are compliance or mandated by CPUC or other agencies are listed in bold; Appendix C attached to this testimony provides the details regarding these mandates for each control.

TABLE OZ-10
SoCalGas RAMP and GRC Risk Control/Mitigation Activities - O&M

Cybersecurity				
ID	**Control/Mitigation Name**	**2025 RAMP 2028-2031 In 2024$ (000s)**	**2028 GRC 2028-2031 In 2025$ (000s)**	**Change ($000s)**
C801	**Perimeter Defenses**	$17,084	$2,595	($14,500)
C802	**Internal Defenses**	$35,932	$32,839	($3,093)

TABLE OZ-11
SDG&E RAMP and GRC Risk Control/Mitigation Activities - O&M

Cybersecurity				
ID	**Control/Mitigation Name**	**2025 RAMP 2028-2031 In 2024$ (000s)**	**2028 GRC 2028-2031 In 2025$ (000s)**	**Change ($000s)**
C801	**Perimeter Defenses**	$5,834	$7,569	$1,735
C802	**Internal Defenses**	$42,450	$45,487	$3,037
C803	**Sensitive Data Protection**	$2,108	$2,428	$320

B. Description of Selection and Prioritization of RAMP Risk Mitigations

The RAMP risk mitigation efforts are associated with specific actions, such as programs, projects, processes, and utilization of technology and are designed to address a specific safety and/or reliability risk. The Companies' selection and prioritization of these RAMP mitigation activities considered many aspects when determining if these risk mitigation activities are an effective and worthwhile investment. The Enterprise Risk Management (ERM) process for identifying and assessing system risk is described in the RDF Integration testimony (Ex. SCG-02B/SDGE-02B).

In selecting and prioritizing cybersecurity RAMP mitigations funded through O&M, the Companies apply a risk-based operational review consistent with the Enterprise Risk Management framework described in the RDF Integration testimony (Ex. SCG-02B/SDGE-02B). O&M mitigations are focused on sustaining, operating, and enforcing cybersecurity controls and processes that address identified safety and reliability risks on a recurring basis.

The Cybersecurity organization evaluates O&M mitigation activities based on several considerations, with primary emphasis on: (1) the degree to which the activity supports continuous risk reduction by maintaining or enhancing the effectiveness of existing controls; (2) whether the activity is required to meet legal, regulatory, or compliance obligations; (3) the operational workload created by threat activity, system scale, data volume, or regulatory requirements; and (4) the ability to execute the activity without introducing operational disruption or degrading system reliability. Cost reasonableness is considered in this context to ensure that requested O&M resources are proportional to the sustained workload and risk addressed.

O&M mitigations are prioritized when they are necessary to operate and sustain previously authorized cybersecurity investments, respond to measurable increases in cybersecurity workload, or maintain compliance with evolving regulatory requirements. Activities may be deferred or not selected when existing controls already address the risk, when incremental risk reduction is limited, or when the activity would create undue operational burden without a corresponding benefit to safety or reliability.

O&M cybersecurity mitigations strive to support safe and reliable electric and gas service for customers through reducing the likelihood and impact of cybersecurity events that could disrupt operations, impair service delivery, or compromise sensitive customer information. These activities also help prevent the growth of future risk by ensuring that foundational cybersecurity capabilities remain effective as threats, systems, and regulatory expectations evolve.

VI. CAPITAL

Table OZ-12 summarizes capital forecasts for 2026 through 2031. The particular in-service date for the capital expenditures that underly these forecasts is provided in workpapers. Appendix D to this testimony provides a table that illustrates the capital expenditures that are estimated to have in-service dates between 2026 and Test Year

2028. Capital expenditures that are in-service between 2026-2028 will contribute to the Test Year 2028 revenue requirement request presented in the Summary of Earnings testimony (Ex, SCG-27 and Ex, SDGE-32). Capital expenditures with in-service dates in the post-test years (i.e., 2029-2031) are also included in Appendix D. The post-test year revenue requirement request is included in the Post-Test Year Ratemaking testimony (Ex. SCG-28 and Ex, SDGE-33).

O&M funding, discussed in sections III and IV, supports the ongoing operation, maintenance, and continuous execution of cybersecurity activities necessary to sustain these capabilities and respond to the evolving threat environment on a day-to-day basis. In contrast, capital expenditures fund the acquisition, development, and implementation of new or enhanced cybersecurity technologies and infrastructure that provide multi-year risk mitigation benefits, including system upgrades, platform deployments, and capability expansions.

Planning for cybersecurity risk mitigation is particularly challenging because of the wide range of potential risk drivers, including rapid changes in technology, innovations in business capabilities, evolving threats in terms of sophistication, automation, aggressiveness, and increasing system interdependencies. Cybersecurity risk cannot be completely mitigated or avoided; however, the Companies can manage it by following well understood principles, implementing cyber leading practices, and keeping pace with changing threats.

All foundational capital activities will continue to be performed. However, due to the evolving nature of the threats associated with this risk, if only current activities were maintained, the level of risk would likely grow. Accordingly, the Companies are looking to new processes and technologies to improve or replace existing security capabilities to address the ever-changing threats landscape. While it is possible to plan for technology refresh costs based on the useful lifetime of a solution, as considered by the Infrastructure and Platform Security Lifecycle capital activities, it is difficult to accurately predict unforeseen cybersecurity costs, like those incurred with the Cybersecurity program, in response to changes in threat capabilities that prematurely make a technology obsolete or require the use of a new technical control.

The Cybersecurity Program continually reassesses planned capital activities based on current cybersecurity risks. Due to risk management adjustments, planned activities are continually reprioritized and restructured. Also, activities may happen in different years than planned due to changes in priority and resource availability as a result of the continuous

reassessment of threats, known risks, and prioritization. Table OZ-12 summarizes the total capital forecasts for 2026, 2027, 2028, 2029, 2030, and 2031.

TABLE OZ-12

SDG&E Capital Expenditures Summary of Costs

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
1. PERIMETER DEFENSES	8,303	0	1,638	2,740	813	5,280	7,920
2. INTERNAL DEFENSES	5,470	0	3,526	9,444	0	5,280	1,491
3. SENSITIVE DATA PROTECTION	18,402	0	0	4,110	0	7,920	0
4. OPERATIONAL TECHNOLOGY CYBERSECURITY	329	0	3,526	8,093	3,848	3,972	9,149
5. INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	0	0	0	2,740	0	6,365	1,086
6. EMERGING THREAT DEFENSES	0	0	0	6,691	0	2,640	5,289
Total	**32,504**	**0**	**8,690**	**33,818**	**4,661**	**31,457**	**24,935**

TABLE OZ-13
SoCalGas Capital Expenditures Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
1. PERIMETER DEFENSES	35,914	7,094	9,318	9,811	6,367	25,080	46,368
2. INTERNAL DEFENSES	12,589	30,173	13,068	22,691	25,461	13,694	37,563
3. SENSITIVE DATA PROTECTION	23,474	5,674	2,614	41,060	7,623	16,834	8,712
4. OPERATIONAL TECHNOLOGY CYBERSECURITY	4,329	2,365	10,810	12,983	16,039	5,303	14,597
5. INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	7,183	2,828	7,619	3,440	1,633	7,807	1,088
6. EMERGING THREAT DEFENSES	0	1,238	7,619	13,027	8,363	19,474	12,771
Total	**83,489**	**49,372**	**51,048**	**103,012**	**65,486**	**88,192**	**121,099**

A. SDG&E & SoCalGas

1. Forecast Method

SoCalGas and SDG&E cybersecurity capital projects use a zero-based forecast methodology because historical spending patterns are not a reliable predictor of future cybersecurity needs. The cybersecurity capital portfolio changes materially from year to year due to evolving threats, short technology lifecycles, vendor end of support timelines, and changing regulatory and risk conditions. As a result, projects are frequently added, modified, deferred, or replaced, limiting the usefulness of base year or historical average forecasting.

While some cybersecurity capital reflects routine lifecycle sustainment, a substantial portion consists of non-routine, risk driven initiatives that respond to emerging threats, new requirements, and technology obsolescence. These non-routine investments do not recur predictably and cannot be accurately forecasted using historical averages, which would understate future needs. In this context, a zero-based approach provides a more accurate and reasonable forecast by evaluating each planned project based on current risk conditions, expected threat evolution, and implementation requirements. Detailed cost estimates are developed by experienced internal and external personnel, where applicable, and are informed by current market quotes, vendor proposals, and prevailing industry conditions for cybersecurity technologies and services.

2. Perimeter Defenses

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Perimeter Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $7.1M, $9.3M, $9.8M, $6.4M, $25.1M, and $46.4M, respectively. The SDG&E forecast for Perimeter Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $1.6M, $2.7M, $0.8M, $5.3M, and $7.9M, respectively. The Companies plan to build and place in service Perimeter Defenses by the Test Year. Modern perimeter defense focuses on securing the network edge with adaptive, layered controls rather than static barriers. The Perimeter Defenses program includes activities that the Companies take to protect the external access points of their internal information technology systems. Perimeter Defenses are designed to prevent attacks, protect the integrity of, and detect unauthorized access to the Companies' internal information technology systems. The information technology environment includes the entire business technology system, including email, information storage, billing and customer records, among others. The OT environment also uses Perimeter Defenses to protect operational technology assets.

A robust set of controls at the perimeter of corporate systems contributes to the Companies' defense-in-depth strategy. A defense-in-depth strategy manages risk with diverse defenses so that if one layer of defense turns out to be inadequate, the additional layers of defense will prevent and detect further impacts and/or a potential breach. Perimeter Defenses are an important component of defense-in-depth but can only reduce the probability of an adversary having unauthorized access to internal systems and data. This activity includes enhancements to

firewalls and other intrusion protection measures to maintain the risk at the current manageable level and keep up with the increasing potential threats to the perimeter. Perimeter defenses reduce the likelihood of successful external attacks by controlling and monitoring access at the network edge. This strategy limits entry and exit to authorized users, decreases the chance that malicious code will penetrate the environment, and introduces barriers that slow or deter attackers. It also provides visibility into all ingress and egress points while enabling continuous real-time monitoring of perimeter activity.

The activities under this area address risks such as data manipulation or integrity failures, infrastructure outages, unauthorized access, malicious software intrusions, cybersecurity control breakdowns, operational system disruptions, equipment loss or theft, and human error. By implementing strong perimeter defenses, organizations reduce the potential impact of data corruption, system unavailability, theft or destruction of assets, and exposure of sensitive business information including customer records. Examples of capital activities under Perimeter Defenses include:

- Upgrading firewalls, web-application firewalls, and related perimeter security technologies to strengthen protection at external access points.
- Implementing distributed-denial-of-service (DDoS) protections and other perimeter-level threat-mitigation technologies that improve filtering, inspection, and intrusion prevention capabilities.
- Enhancing tools that control and monitor ingress and egress traffic to reduce the likelihood of unauthorized access and improve real-time visibility into network-edge activity.
- Investing in perimeter controls that apply to both IT and OT environments to protect operational systems, maintain system integrity, and reduce the consequences of data manipulation, system outages, or unauthorized access.

Information regarding Perimeter Defense is found in the capital workpapers, Ex. SCG-11-CWP (A07450.0)/ SDGE-15-CWP (00906A.000). Perimeter Defenses mitigate safety risks identified in the 2025 RAMP Report, Chapter SCG-RISK-8/SDGE-RISK-8, Cybersecurity, and aligns with RAMP Activity C801 Perimeter Defenses.

TABLE OZ-14
SDG&E Capital Expenditures Summary of Costs – Perimeter Defenses

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
1. PERIMETER DEFENSES	8,303	0	1,638	2,740	813	5,280	7,920

TABLE OZ-15
SoCalGas Capital Expenditures Summary of Costs – Perimeter Defenses

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
1. PERIMETER DEFENSES	35,913	7,094	9,318	9,811	6,367	25,080	46,368

b. Cost Drivers

The underlying cost drivers for Perimeter Defenses are risk mitigation activities driven by the evolving and increasingly sophisticated tools and strategies threat actors use to conduct attacks on the energy sector. Cybersecurity's Perimeter Defense capital costs are driven by non-labor costs for hardware and software for cybersecurity systems and contractor services, and labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were included in the Cybersecurity forecast to more accurately reflect their direct role in protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology market. Due to the cyclical nature of multi-year licensing payment structures, annual costs vary.

Renewal years are higher than non-renewal years, resulting in an unevenness in annual forecasted spend.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technologies or vendors. These cost increases are entirely outside the utilities' control and reflect broader market conditions affecting critical infrastructure operators.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (A07450.0)/SDG&E-15-CWP (00906A.000).

3. Internal Defenses

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Internal Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $30.2M, $13.1M, $12.5M, $25.4M, $13.7M, and $37.6M, respectively. The SDG&E forecast for Internal Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $3.5M, $9.4M, $0M, $5.3M, and $1.5M, respectively. The Companies plan to build and place in service Internal Defenses by the Test Year. Internal Defense program activities are designed to detect and prevent unauthorized users, those misusing authorized credentials and malicious software (*e.g.*, malware) from propagating inside of the perimeter, and moving within the IT system or into the OT system. These enhancements to the Companies' IT and OT systems' Access Management system reduce the risk to internal systems and the likelihood and impact of a Cybersecurity incident.

As another layer of defense-in-depth, the activities within this category include investments that directly strengthen controls and protections of internal assets and internal information. The activities in this area are designed to detect unauthorized users from moving laterally or vertically within the IT system or into the OT system, enabling a faster response to threats. The enhancements to the IT and OT systems' Access Management system allow the Companies to keep the current risk level steady.

Examples of capital activities under Internal Defenses include:

- Upgrading identity and access management technologies to reduce the risk of unauthorized or malicious use of credentials within IT and OT environments.
- Enhancing endpoint-security monitoring, threat and vulnerability management capabilities, and incident-response systems used to detect and contain activity that bypasses perimeter controls.
- Deploying tools that help prevent lateral movement within internal networks and improve the ability to identify anomalous user or system behavior.
- Strengthening internal protections through investments in cloud-security capabilities, third-party and supply-chain risk controls, and monitoring technologies with embedded analytics that improve alert correlation and response efficiency.
- Enhancements to platforms that support user behavior reinforcement tied to Internal Defense controls, e.g. user notifications to educate on cyber safe behavior-based system monitoring for risk events.

As part of the evolution of technology, many vendors are providing enhancements embedding artificial intelligence and machine learning capabilities to existing products deployed. There are cybersecurity risks that must be assessed and mitigated for this new functionality. Cybersecurity is enhancing capabilities including behavioral anomaly detection, automated alert correlation and prioritization, and limited automated response actions within endpoint, identity, and security monitoring platforms to defend against these new and developing threats.[57]

Information regarding Internal Defenses is found in the capital workpapers. *See* Ex. SDG&E-28-OZ 00906B.000 – Internal Defenses and SCG-28-OZ B07450.0. Internal Defenses mitigates safety risks identified in the 2025 RAMP Report, Chapter SCG-RISK-8/SDGE-RISK-8, Cybersecurity and aligns with RAMP activity C802 Internal Defenses.

[57] By contrast, the Emerging Threat Defenses mitigation described elsewhere in this testimony specifically addresses advanced threats posed by adversaries' use of AI and other emerging technologies, as well as risks introduced by the internal adoption of AI, and is therefore scoped separately.

TABLE OZ-16
SDG&E Capital Expenditures Summary of Costs – Internal Defenses

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
2. INTERNAL DEFENSES	5,470	0	3,526	9,444	0	5,280	1,491

TABLE OZ-17
SoCalGas Capital Expenditures Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
2. INTERNAL DEFENSES	12,589	30,173	13,068	22,691	25,461	13,694	37,563

b. Cost Drivers

The underlying cost drivers for Internal Defenses are risk mitigation activities driven by the evolving and increasingly sophisticated tools and tactics threat actors use to conduct attacks on the energy sector. Cybersecurity's Internal Defenses capital costs are driven by non-labor costs for hardware and software materials for cybersecurity systems and contractor services and labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were included in the cybersecurity forecast to more accurately reflect their direct role in protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology supply chain and vendor market, including impacts related to system setup, implementation, and licensing. Due to the cyclical nature of multi-year licensing payment structures, annual costs

vary. Renewal year costs are higher than non-renewal year costs, resulting in an unevenness in annual forecasted spend.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost drivers are seen across mitigation areas, as certain capital technology investments support multiple types of mitigations and controls, including the specific capabilities and activities described in this section. These cost increases are entirely outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (B07450.0)/SDGE-15-CWP (00906B.000).

4. Sensitive Data Protections

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Sensitive Data Protections for 2026, 2027, 2028, 2029, 2030, and 2031 are $5.7M, $2.6M, $41.1M, $7.6M, $16.8M, and $8.7M, respectively. The SDG&E forecast for Sensitive Data Protections for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $0M, $4.1M, $0M, $7.9M, and $0M, respectively. The Companies plan to build and place in service Sensitive Data Protection by the Test Year. Sensitive Data Protection is a core component of the Companies' defense-in-depth strategy for cybersecurity. The Sensitive Data Protection projects outlined below enhance technology to reduce the risk of unauthorized access to sensitive data by understanding where sensitive data is stored, how it is transmitted, and how it is used. This helps to further protect customer and Company information and reduce the risk of data corruption, data breaches, unauthorized disclosure of sensitive information, and non-compliance. The activities for this area will help the Companies continue the prudent management of sensitive data. The Companies' current activities are focused on sensitive data within information technology systems, such as laptops and other mobile computing devices. Examples of capital activities under Sensitive Data Protection include:

- Procuring and deploying cybersecurity hardware, software, and contracted services needed to secure sensitive customer, employee, and Company information.
- Implementing system enhancements that improve protection against increasingly sophisticated tools used to compromise sensitive data, including upgrades required to meet evolving cybersecurity and privacy regulations.
- Investing in platforms, compute resources, and licensing needed to support secure processing, storage, and transmission of sensitive data across IT and OT environments.
- Performing technology refreshes and upgrades that ensure continued effectiveness of data-protection systems as vendors change licensing models, retire older technologies, or introduce new capabilities needed to address modern threats.

These activities strengthen controls to mitigate the risk of unauthorized access to sensitive systems and information, reduce the likelihood that confidential data is improperly shared or transmitted outside the organization, enhance protections for Company-issued devices in the event of loss, theft, or compromise, and inventory sensitive information across the Companies' systems to facilitate implementation of appropriate safeguards. Collectively, these measures enhance the Companies' ability to prevent unauthorized access, limit potential exposure, and proactively manage risks to customer, employee, and Company data.

Information regarding Sensitive Data Protection is found in my capital workpapers, Ex. SCG-28-CWP (E07450.0)/SDGE-15-CWP (00906C.000). Sensitive Data Protection mitigates safety risks identified in the 2025 RAMP Report, Chapter SCG-RISK-8/SDGE-RISK-8, Cybersecurity, and aligns with RAMP activity C03 Sensitive Data Protection.

TABLE OZ-18
SDG&E Capital Expenditures Summary of Costs – Sensitive Data Protection

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
3. SENSITIVE DATA PROTECTION	18,402	0	0	4,110	0	7,920	0

TABLE OZ-19
SoCalGas Capital Expenditures Summary of Costs – Sensitive Data Protection

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
3. SENSITIVE DATA PROTECTION	23,474	5,674	2,614	41,060	7,623	16,834	8,712

b. Cost Drivers

The underlying cost drivers for Sensitive Data Protection are risk mitigation activities driven by the evolving and increasingly sophisticated tools and strategies threat actors use to conduct attacks on the energy sector. Cybersecurity's Sensitive Data Protection capital costs are driven by non-labor costs for hardware and software materials for cybersecurity systems and contractor services and labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were included in the Cybersecurity forecast to more accurately reflect their direct role in protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology market.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost increases are entirely outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators. Due to the cyclical nature of multi-year licensing payment structures, annual costs vary. Renewal year costs are higher than non-renewal year costs, resulting in an unevenness in annual forecasted spend.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (E07450.0)/SDG&E-15-CWP (00906C.000).

5. Operational Technology (OT) Cybersecurity

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Operational Technology (OT) Cybersecurity for 2026, 2027, 2028, 2029, 2030, and 2031 are $2.4M, $10.8M, $13M, $16M, $5.3M, and $14.6M, respectively. The SDG&E forecast for OT Cybersecurity for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $3.5M, $8.1M, $3.8M, $3.9M, and $9.1M, respectively. The Companies plan to build and place in service OT Cybersecurity by the Test Year. The OT Cybersecurity program focuses on securing the Companies' electric and gas control systems that manage the flow of energy. OT environments enable critical business functions, including safe and reliable energy delivery to customers throughout the service territory. As the penetration of DER, system sensors, and digitally connected devices continues to increase throughout the Companies' territory, the OT target surface grows significantly, since more two-way communication devices, each a potential entryway to the Companies network, are connected to the Companies' grid infrastructure.

Cybersecurity requires a specialized approach to meet operational needs while also providing strong cybersecurity risk mitigation and controls. Improving asset management helps identify unauthorized systems, which may include any computer, device, software application or network components that connect to the Companies' IT or OT network, which could potentially be a source of an attack. Network anomaly detection, endpoint detection, and security event monitoring improve visibility in the OT environment, which allows for faster response and

remediation. Enhanced secure access technologies help reduce the risk of unauthorized access. These activities strengthen the Companies' capabilities by securing the foundation of OT security. These enhancements are necessary to sustain a secure OT system, as operational needs become more advanced and complex, and mitigate the increasing potential threat on critical systems.

The Companies' cybersecurity program prioritizes operational technology activities, including: the management of its existing technology assets, improving threat intelligence and vulnerability management, and securing the network communication infrastructure, including but not limited to advanced metering infrastructure (AMI), field sensors, and Supervisory and Data Acquisition (SCADA[58]) technology. The Companies are focused on maintaining a secure operational environment to support safe, reliable gas and electric systems and service.

The types of OT Cybersecurity activities include efforts in the OT environment (including ICS[59] and SCADA) such as:

- Identifying unauthorized systems and devices connected to IT and OT networks through improved asset management and discovery.
- Implementing and operating OT-focused controls such as network segmentation, multifactor authentication, network anomaly detection, and advanced security event monitoring.
- Deploying and operating OT-specific protections including SIEM and analytics, network access control, endpoint detection and response, malware defense, and secure remote connection capabilities in environments such as ICS and SCADA.

Information regarding OT Cybersecurity is found in my capital workpapers, Ex. SCG-11-CWP (C07450.0)/SDG&E-15-CWP (00906D.000). OT Cybersecurity mitigates safety risks identified in the 2025 RAMP Report, Chapter SCG-RISK-8/SDGE-RISK-8, Cybersecurity, and aligns with RAMP activity C804 OT Cybersecurity.

[58] Supervisory Control and Data Acquisition: systems used to monitor and control utility infrastructure operations.

[59] Industrial control system (ICS) is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

TABLE OZ-20
SDG&E Capital Expenditures Summary of Costs – OT

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
4. OPERATIONAL TECHNOLOGY CYBERSECURITY	329	0	3,526	8,093	3,848	3,972	9,149

TABLE OZ-21
SoCalGas Capital Expenditures Summary of Costs – OT

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
4. OPERATIONAL TECHNOLOGY CYBERSECURITY	4,329	2,365	10,810	12,983	16,039	5,303	14,597

b. Cost Drivers

The underlying cost drivers for Operational Technology Cybersecurity are risk mitigation activities driven by the evolving and increasingly sophisticated tools and tactics threat actors use to conduct attacks on the energy sector. Cybersecurity's operational technology capital costs are driven by non-labor costs for hardware and software for cybersecurity systems and contractor services, including labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were included in the Cybersecurity forecast to more accurately reflect their direct role in protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology market. Due to the cyclical nature of multi-year licensing payment

structures, annual costs vary. Renewal year costs are higher than non-renewal year costs, resulting in an unevenness in annual forecasted spend.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost increases are entirely outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (C07450.0)/SDGE-15-CWP (00906D.000).

6. Infrastructure and Platforms Security Lifecycle Management

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Infrastructure and Platforms Security Lifecycle Management for 2026, 2027, 2028, 2029, 2030, and 2031 are $2.8M, $7.6M, $3.4M, $1.6M, $7.8M, and $1.1M, respectively. The SDG&E forecast for Infrastructure and Platforms Security Lifecycle Management for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $0M, $2.7M, $0M, $6.4M, and $1.1M, respectively. In Cybersecurity's recent RAMP filing, this mitigation area was titled IT Infrastructure Modernization. The cybersecurity risk focus of this program is more expansive than the title would suggest. The primary objective is reduction of cyber risk associated with end-of-support technologies and security obsolescence, rather than general IT modernization. These conditions create exploitable vulnerabilities that can compromise the integrity and resilience of critical systems supporting electric and gas operations. By mitigating exploitable vulnerabilities, the Companies are supporting mitigation of safety risks identified in RAMP and helping preserve system and service reliability through avoidance of disruptions to daily system operations.

The updated name used in this testimony, Infrastructure and Platforms Security Lifecycle Management, better reflects the program's purpose and alignment with Commission priorities related to system safety, reliability, and risk-based mitigation of safety-related threats. These priorities are reflected in the CPUC Safety Policy Division's Evaluation Report on Sempra's 2025 RAMP Applications (A.25-05-010), which emphasizes risk-based mitigation of

safety-related threats, system reliability, and lifecycle management of technology to reduce cybersecurity risk. In particular, this area underscores:

- Security as the driver: The lifecycle refresh of technology is undertaken to maintain supported-state security controls and prevent exposure from outdated platforms.
- Risk mitigation, not modernization: This is a cybersecurity control strategy designed to reduce threats, not an IT upgrade initiative.
- Lifecycle discipline: The name signals structured management of technology and security lifecycles, consistent with industry best practices and the expectations reflected in the CPUC Safety Policy Division's Evaluation Report on Sempra's 2025 RAMP Applications (A.25-05-010). This change establishes clarity for stakeholders and the Commission that the infrastructure and platforms security lifecycle management is a core cybersecurity mitigation measure tied to reliability and safety, rather than discretionary IT improvements. Technology lifecycles – especially in the cybersecurity realm – are short, requiring frequent upgrades to patch vulnerabilities within legacy technology, and to also avoid security obsolescence, a process that refers to cybersecurity tools and processes that are no longer effective or could potentially create new vulnerabilities. Vulnerabilities inherent in legacy technology can provide a foothold for entry or movement within the Companies' environment. Failure to invest in modern technologies could degrade the value of modern investments due to compatibility restrictions. Replacing legacy technology is a necessary method of managing cybersecurity risk.

The Infrastructure and Platforms Security Lifecycle Management activities include technology refreshes and/or replacements of obsolete infrastructure, operating systems, middleware and applications that are specific to cybersecurity tooling and capabilities, as opposed to technology for IT or business needs. Additionally, there is a need to provide ongoing system maintenance activity to confirm continued secure configurations, patching, and upgrading, among others. The Companies are continuing to invest in platforms that can enable more efficient sustainment of security configurations, as demonstrated in the Information Technology testimony (Ex. SCG-10/SDGE-14). Lastly, the need to utilize effective architecture

and other mechanisms to confirm high availability and service continuity for critical systems' reliability. Examples of Infrastructure and Platforms Security Lifecycle Management activities include:

- Replacing or upgrading cybersecurity tools and platforms when vendor end-of-support or technology obsolescence creates increased risk.
- Performing lifecycle sustainment tasks—such as patching, configuration management, and capacity upgrades—to keep core cybersecurity capabilities effective.
- Managing compute resources and enterprise licensing costs that have been realigned to the Cybersecurity forecast to reflect their direct role in protecting critical infrastructure, OT environments, and sensitive data.

This mitigation area addresses lifecycle and obsolescence risk for cybersecurity platforms themselves and does not duplicate other mitigation areas, which fund functional security controls rather than the supported state infrastructure those controls require, nor technology lifecycle management included in the Information Technology forecast (Ex. SCG-10/SDGE-14).

Information regarding Infrastructure and Platforms Security Lifecycle Management is found in the capital workpapers, Ex. SCG-11-CWP (007450.0)/SDG&E-15-CWP (00906E.000) Infrastructure and Platforms Security Lifecycle Management mitigates safety risks identified in the 2025 RAMP Report, Chapter SCG-RISK-8/SDGE-RISK-8, Cybersecurity, and aligns with RAMP activity C805 Obsolete IT Infrastructure and Application Replacement.

TABLE OZ-22
SDG&E Capital Expenditures Summary of Costs

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
5. INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	0	0	0	2,740	0	6,365	1,086

TABLE OZ-23
SoCalGas Capital Expenditures Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
5. INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	7,183	2,828	7,619	3,440	1,633	7,807	1,088

b. Cost Drivers

The underlying cost drivers for Infrastructure and Platforms Security Lifecycle Management are risk mitigation activities driven by the evolving and increasingly sophisticated tools and tactics threat actors use to conduct attacks on the energy sector. Cybersecurity's infrastructure and platforms security lifecycle management capital costs are driven by non-labor costs for hardware and software for cybersecurity systems and contractor services, including

labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which were included in the Cybersecurity forecast to more accurately reflect their direct role in protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology market. Due to the cyclical nature of multi-year licensing payment structures, annual costs vary. Renewal year costs are higher than non-renewal year costs, resulting in an unevenness in annual forecasted spend.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal costs, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost increases are entirely outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (007450.0)/SDGE-15-CWP (00906E.000).

7. Emerging Threat Defenses

a. Description of Costs and Underlying Activities

The SoCalGas forecast for Emerging Threat Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $1.2M, $7.6M, $13M, $8.4M, $19.5M, and $12.8M, respectively. The SDG&E forecast for Emerging Threat Defenses for 2026, 2027, 2028, 2029, 2030, and 2031 are $0M, $0M, $6.7M, $0M, $2.6M, and $5.3M, respectively. The Companies plan to build and place in service Emerging Threat Defenses by the Test Year. Overall, emerging threat defenses are preemptive risk mitigation methods that protect against advanced cyber threats that exceed the detection and response capabilities of legacy systems and traditional mitigations. With the advancements in artificial intelligence and quantum computing over the last few years, the Companies need to be ready to detect and defend against new types of attacks that may be more sophisticated and prevalent than those seen in recent years, as indicated by 2025 RAMP Bow Tie

Drivers/Triggers DT.9 Emerging Threats.[60]

The types of activities included under Emerging Threat Defenses encompass specialized cybersecurity efforts designed to counter advanced and unconventional threats that traditional systems cannot reliably detect or contain, such as deepfakes, advanced social engineering, quantum decryption, and AI vulnerability exploitation, as well as other cybersecurity threats that will emerge as part of the evolving global cyber threat environment and cannot be fully anticipated at this time. These efforts are implemented across both IT and OT environments to support business continuity and reduce exposure to high-impact cyber risks and address current increases in workload associated with advanced threat techniques identified in the 2025 RAMP. Key efforts include:

- Deployment of AI-driven threat detection, monitoring, response systems
- Zero-day exploit[61] containment technologies
- Disinformation and threat-intelligence monitoring
- Threat intelligence fusion and automation engines
- Behavioral analytics for adversarial pattern recognition
- Preliminary establishment of quantum-resilient cryptographic protocols

These activities form a cohesive defense strategy that adapts to new and evolving cyber threats. AI-enabled analytics provide the ability to identify subtle anomalies and correlate threat indicators across complex IT and OT environments much faster than manual processes, which is critical as attackers increasingly use automation and advanced methods to evade traditional controls. These capabilities support earlier detection of potential intrusions, faster containment of malicious activity, and more efficient prioritization of vulnerabilities and risks. Integrating AI into cybersecurity operations aligns with the RAMP-identified need for controls that continually evolve as threats,[62] supporting our defensive capabilities to remain resilient against increasingly

---

[60] CPUC – Safety Policy Division, *Evaluation Report on Sempra's 2025 RAMP Applications (A.)25-05-10* (October 10, 2025) at 176, *available at*: https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/safety-policy-division/reports/safety-policy-division-evaluation-report-on-sempras-2025-ramp-applications.pdf.

[61] Zero-Day Exploit: the use of a previously unknown vulnerability to gain unauthorized access or disrupt systems before a mitigation is available.

[62] *Id.*

sophisticated adversaries and reducing the likelihood and consequence of disruptive high-complexity cyber events.

Activities funded under this area address a wide range of potential cybersecurity consequences, including manipulated data or integrity failure, infrastructure or availability failure, access control or confidentiality failure, malicious software intrusions, cybersecurity control failures, operational system failures, equipment loss or theft, human error, data corruption or unavailability, theft or destruction of systems and data, and exposure of sensitive business information including customer records.

Information regarding Emerging Threat Defenses is found in my capital workpapers. Ex, SCG-11-CWP (007450.0)/SDGE-15-CWP (00906F.000). Emerging Threat Defenses addresses the following Drivers/Triggers: DT.2: Advanced Persistent Threats (APT[63]OBJ, DT.4: Malware and Malicious Software, DT.8: Cybersecurity Control Failures, DT.9: Emerging Threats, DT.10: Safety-Critical Cyber Risks and mitigates safety risks identified in the 2025 RAMP Report, including the following potential consequences:

- PC.2: Data corruption or unavailability
- PC.3: Theft or destruction of systems/data
- PC.4: Exposure of sensitive Company and/or customer data
- PC.6: Erosion of public confidence
- PC.8: Serious injuries and/or fatalities

[63] Advanced Persistent Threat (APT): a prolonged and targeted cyberattack in which an unauthorized actor gains and maintains access to a network in order to exfiltrate data, disrupt operations, or compromise systems over time.

TABLE OZ-24
SDG&E Capital Expenditures Summary of Costs

SDG&E CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
6. EMERGING THREAT DEFENSES	0	0	0	6,691	0	2,640	5,289

TABLE OZ-25
SoCalGas Capital Expenditures Summary of Costs

SoCalGas CYBERSECURITY (In 2025 $)							
A. CYBERSECURITY	**2025 Adjusted-Recorded (000s)**	**Est. 2026 (000s)**	**Est. 2027 (000s)**	**Est. 2028 (000s)**	**Est. 2029 (000s)**	**Est. 2030 (000s)**	**Est. 2031 (000s)**
6. EMERGING THREAT DEFENSES	0	1,238	7,619	13,027	8,363	19,474	12,771

b. Cost Drivers

The underlying cost drivers for Cybersecurity's capital categories are risk mitigation activities driven by the evolving and increasingly sophisticated tools and tactics threat actors use to conduct attacks on the energy sector. These activities are designed to enhance our perimeter defenses, internal defenses sensitive data protection, OT cybersecurity, Infrastructure and Platforms Security Lifecycle Management and emerging threat defenses. Cybersecurity's capital costs are driven by non-labor costs for hardware and software materials for cybersecurity systems and contractor services, including the transfer of and labor costs for the employees assigned to design, build, and deploy new systems. Additional cost drivers reflect realignment of certain costs as cybersecurity, including compute processing power and enterprise licensing costs which included in the Cybersecurity forecast to more accurately reflect their direct role in

protecting critical infrastructure, operational technology environments, and sensitive data along with changes in the cybersecurity technology market. Due to the cyclical nature of multi-year licensing payment structures, annual costs vary. Renewal years are higher than non-renewal years, resulting in an unevenness in annual forecasted spend.

In addition, the cost of core cybersecurity capabilities has increased materially since the prior GRC filing period. These increases are driven by shifts in vendor licensing models or renewal cost, the need for expanded capabilities to address a more sophisticated threat landscape, accelerating AI adoption, and limited flexibility to competitively price or evaluate alternatives due to dependencies on certain technology or limited vendor choice. These cost increases are outside the Companies' control and reflect broader market conditions affecting critical infrastructure operators.

Documentation of these cost drivers are included as supplemental capital workpapers, Ex. SCG-11-CWP (E07450.0)/SDGE-15-CWP (00906F.000).

VII. RAMP INTO GRC - CAPITAL

A. Description of RAMP Mitigations

The capital activities described above in Section VI were also presented in the 2025 RAMP Report and are listed in the tables below. Activities that are compliance or mandated by CPUC or other agencies are listed in bold; Appendix C attached to this testimony provides the details regarding these mandates for each control.

TABLE OZ-26
SoCalGas RAMP and GRC Risk Control/Mitigation Activities – Capital

Cybersecurity				
ID	**Control/Mitigation Name**	**2025 RAMP 2028-2031 In 2024$ (000s)**	**2028 GRC 2028-2031 In 2025$ (000s)**	**Change ($000s)**
C801	**Perimeter Defenses**	58,425	87,626	29,201
C802	**Internal Defenses**	84,653	99,409	14,756
C803	**Sensitive Data Protection**	9,720	74,229	64,509
C804	**Operational Technology (OT) Cybersecurity**	16,929	48,922	31,993
C805	**Infrastructure and Platforms Security Lifecycle Management**[64]	11,377	13,968	2,591
M811	Emerging Threat Defenses[65]	n/a	53,635	53,635

TABLE OZ-27
SDG&E RAMP and GRC Risk Control/Mitigation Activities - Capital

Cybersecurity				
ID	**Control/Mitigation Name**	**2025 RAMP 2028-2031 In 2024$ (000s)**	**2028 GRC 2028-2031 In 2025$ (000s)**	**Change ($000s)**
C801	**Perimeter Defenses**	n/a	16,753	16,753
C802	**Internal Defenses**	2,873	16,215	13,342
C803	**Sensitive Data Protection**	$0	12,030	12,030
C804	**Operational Technology (OT) Cybersecurity**	14,800	25,062	10,262
C805	**Infrastructure and Platforms Security Lifecycle Management**[66]	10,000	10,191	$191
M811	Emerging Threat Defenses[67]	n/a	14,620	14,620

B. Description of Selection and Prioritization of RAMP Risk Mitigations

The RAMP risk mitigation efforts are associated with specific actions, such as programs, projects, processes, and utilization of technology and are designed to address a specific safety and/or reliability risk. The Companies' selection and prioritization of these RAMP mitigation

[64] This control was referred to as IT Infrastructure Modernization in the RAMP application.

[65] This mitigation was added after the RAMP application was filed.

[66] This control was referred to as IT Infrastructure Modernization in the RAMP application.

[67] This mitigation was added after the RAMP application was filed.

activities considered many aspects when determining if these risk mitigation activities are an effective and worthwhile investment. The ERM process for identifying and assessing system risk is described in the RDF Integration testimony (Ex. SCG-02B/SDGE-02B).

In selecting and prioritizing cybersecurity RAMP mitigations, the Companies apply a structured, risk-based review aligned with the ERM framework described in the RDF Integration testimony (Ex. SCG-02B/SDGE-02B). For each candidate mitigation, the Cybersecurity organization evaluates the mitigation's alignment to the risk driver and consequence it addresses and prioritizes mitigations that most directly reduce safety and reliability risk.

In prioritizing these mitigations, the Companies place particular emphasis on proactive investments that reduce the likelihood of future cybersecurity events and avoid the significantly higher operational, customer, and recovery impacts associated with responding to realized incidents.

The evaluation typically considers the following factors, in order of emphasis: (1) the severity and materiality of the safety and/or reliability risk addressed, including the extent to which the mitigation reduces the likelihood and/or potential impact of credible cybersecurity events; (2) whether the activity is required to meet applicable legal, regulatory, or compliance obligations; (3) customer and system impacts, including how the mitigation supports safe and reliable service and protects sensitive customer and employee information, and whether implementation can be accomplished while maintaining operational continuity; (4) system and operational constraints, including technical feasibility, implementation complexity, dependencies, and the ability to execute within available resources and schedules; and (5) cost reasonableness and proportionality to the incremental risk reduction achieved.

The Companies' consideration of "cost effectiveness" in this context is a qualitative reasonableness and proportionality review and is distinct from the Benefit-Cost Ratio (BCR) calculations performed under the Risk-Based Decision-Making Framework (RDF) described in the RDF Integration testimony. The purpose of this review is to confirm that the mitigation represents a reasonable investment for the safety and reliability risk addressed, taking into account operational feasibility and customer impacts.

Mitigations may be deferred or not selected when the incremental risk reduction is limited relative to cost, when the mitigation duplicates existing capabilities, when

implementation would create unacceptable operational disruption or reliability risk, or when system constraints make the mitigation infeasible within the planning horizon.

Cybersecurity RAMP mitigations are prioritized to support the Companies' ability to provide safe and reliable electric and gas service by reducing the likelihood and consequences of cybersecurity events that could impair operations or compromise sensitive information. Mitigations that help avoid growth in future risk, including activities that sustain and refresh foundational security capabilities as systems, threats, and requirements evolve, are prioritized to maintain an appropriate risk posture over time.

VIII. RISK ASSESSMENT MITIGATION PHASE (RAMP) INTEGRATION

A. GRC Risk Controls/Mitigations and Benefit Cost Ratios

As previously discussed, certain costs supported in this testimony are for Control/Mitigation activities described in SoCalGas's and SDG&E's May 15, 2025 RAMP Report[68] for activities designed to reduce risk. Specifically, the controls and mitigations in this testimony were included in the 2025 RAMP Report, Chapter SCG-Risk-8/SDG&E-Risk-8, Cybersecurity. As further reference, a roadmap matching controls and mitigations to both the 2025 RAMP and the TY 2028 GRC testimony is appended to Ex. SCG-02B/SDGE-02B. Table OZ-28 below summarizes the Control/Mitigation BCRs based on the costs forecasted[69] in this testimony and estimated in the 2025 RAMP Report with the associated BCRs. Controls/Mitigations that are mandated by CPUC or other agencies are listed in bold in the table below and are listed in Appendix C, attached to this testimony, providing the details regarding the respective mandates for each Control/Mitigation. Appendix E provides a GRC workpaper breakdown for the RAMP controls and mitigations sponsored in this testimony.

[68] A.25-05-010.

[69] Post-test year forecasts can be found in the detailed workpapers Ex. SCG-11/SDGE-15-WP and Ex. SCG-11/SDGE-15-CWP.

TABLE OZ-28
SoCalGas/SDG&E
Comparison of RAMP and GRC Risk Control/Mitigation Benefit Cost Ratios

Cybersecurity							
ID	**Control/ Mitigation Name**	**2025 RAMP Direct, in 2024$ (000s) 2028-2031**			**2028 GRC Direct, in 2025 $ (000s) 2028-2031**		
		BCR Societal	**BCR Hybrid**	**BCR WACC**	**BCR Societal**	**BCR Hybrid**	**BCR WACC**
C801	**Perimeter Defenses**	103.98	97.52	87.83	44.15	43.17	39.50
C802	**Internal Defenses**	33.71	32.54	29.31	15.62	14.80	13.54
C803	**Sensitive Data Protection**	236.7	227.09	204.55	22.94	21.11	19.31
C804	**Operational Technology (OT) Cybersecurity**	220.11	213.21	192.03	54.60	51.57	47.18
C805	**Infrastructure and Platforms Security Lifecycle Management**[70]	197.04	182.04	163.97	83.70	79.20	72.46
M811	Emerging Threat Defenses[71]	n/a	n/a	n/a	58.54	55.54	50.80

B. Justification for Proposed Mitigations With BCRs <1

The RDF describes a methodology for calculating BCRs under multiple discount rates. For the cybersecurity mitigations proposed in this testimony, all calculated BCRs are equal to or greater than one. Accordingly, no proposed mitigations require justification under this section.

C. Changes from 2025 RAMP Report

Since the timing of the filing of the 2025 RAMP Report in May 2025 some circumstances may have changed that impact the control/mitigation scope – including units, costs, and other factors that influence the forecast. In addition, updates may have occurred affecting the underlying assumptions used to calculate the BCRs and are described in the Risk Integration testimony (Ex. SCG-02B/SDGE-02B). Key changes impacting the forecasts include:

- Subsequent to the filing of the 2025 RAMP Report, an additional cybersecurity risk mitigation activity was identified. Per the Safety Policy Division's

[70] This control was referred to as IT Infrastructure Modernization in the RAMP application.

[71] This mitigation was added after the RAMP application was filed.

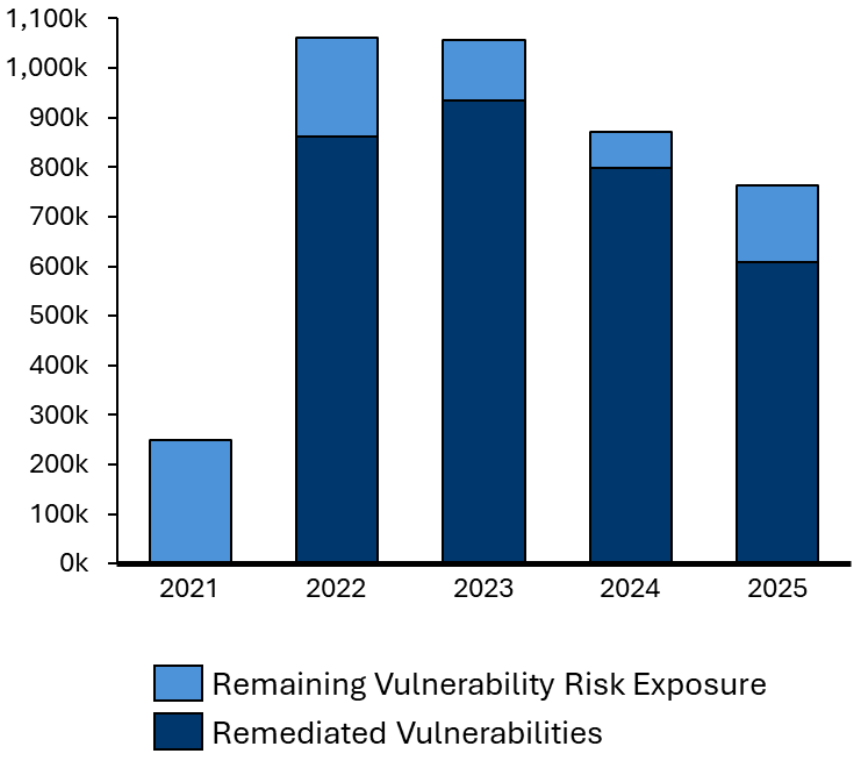
recommendation in its Evaluation Report on Sempra's 2025 RAMP Applications A.25-05-10, the Companies have added Emerging Threat Defenses as a mitigation and have included it as such in this Cybersecurity testimony's capital section. This change has impacted the Cybersecurity capital forecast.

- The nomenclature of Control C805 was changed from IT Infrastructure Modernization to "Infrastructure and Platforms Security Lifecycle Management" to more accurately reflect the cybersecurity-focus of the underlying investments.

D. Feedback from Safety Policy Division and Parties

The Commission's Safety Policy Division (SPD) issued their assessment report on October 10, 2025 regarding the Companies' 2025 RAMP Reports. Parties subsequently served opening and reply comments on November 17, 2025 and December 1, 2025 respectively. Appendix B in the RDF Integration testimony (Ex. SCG-02B/SDG&E-02B, appends a summary of the feedback and recommendations received and the Companies' responses. Pursuant to the March 4, 2026 Administrative Law Judge's Ruling entering the corrected SPD's 2025 RAMP Evaluation Report into the evidentiary record, the Companies have supplemented the Cybersecurity historical progress information to clearly illustrate both "what safety work has been accomplished and what work remains to be done," consistent with D.22-10-002. The corrected SPD report clarifies that historical progress graphics must show completed mitigations as well as remaining work and must align with the RDF. In response, this testimony now includes a vulnerability based historical progress graphic, Figure OZ-6, that displays (1) vulnerabilities remediated during each year, representing safety work accomplished, and (2) the remaining vulnerability backlog, representing work still to be completed in future cycles. This presentation is consistent with the RDF guidelines and reflects SPD's prior feedback incorporated into this chapter.

FIGURE OZ-6
Annual Total Companies' Vulnerabilities Remediated vs. Remaining Backlog



Data is available beginning in 2021

In parallel with vulnerability reduction activities, the Cybersecurity organization continuously manages substantial volumes of malicious activity across perimeter and internal defenses, reinforcing that cybersecurity risk reduction is a sustained operational workload in addition to the discrete mitigations evaluated in RAMP. This vulnerability assessment was conducted at a point in time. As the cybersecurity threat environment is constantly evolving, past vulnerability volumes are not always indicative of future vulnerabilities volumes.

Additionally, in alignment with the Safety Policy Division's recommendation in its Evaluation Report, and to emphasize the area's growing significance as part of the Companies' cybersecurity strategy, the Companies have added Emerging Threat Defenses as a mitigation and have included it in this Cybersecurity testimony's capital section.[72]

[72] CPUC – Safety Policy Division, *Evaluation Report on Sempra's 2025 RAMP Applications (A.)25-05-10* (October 10, 2025) at 176, *available at*: https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/safety-policy-division/reports/safety-policy-division-evaluation-report-on-sempras-2025-ramp-applications.pdf.

IX. CONCLUSION

In summary, the cybersecurity forecasts presented in this testimony reflect prudent, risk-based investments necessary to protect critical gas and electric infrastructure in an environment of increasing threat sophistication, regulatory requirements, and system complexity. The requested O&M and capital expenditures are directly tied to measurable operational workload, compliance obligations, technology lifecycle requirements, and RAMP-aligned risk mitigations, including the newly added mitigation Emerging Threat Defenses. These investments are not discretionary expansions, but rather necessary controls and mitigations required to protect the Companies' assets and customers. The Companies have taken a balanced approach to identify the appropriate level of effort required to sustain effective cybersecurity controls, operate and maintain prior capital investments, and reduce the likelihood and impact of cybersecurity incidents that could affect system reliability, customer data, and public safety. Accordingly, the TY 2028 forecasts are reasonable and necessary to support the Companies' obligation to provide safe, reliable, and resilient service.

This concludes my prepared direct testimony.

X. WITNESS QUALIFICATIONS

My name is Omar Zevallos, and my business address is 8680 Balboa Avenue, San Diego, California 92123. I serve as the Director of Cybersecurity and Chief Information Security Officer (CISO) for SDG&E Enterprise Cybersecurity Technology. In this role, I am responsible for overseeing cybersecurity technology strategy and operations across SDG&E, SoCalGas, and the Corporate Center.

Prior to my current position, I held a range of leadership roles within the organization, including: Field Engineer; Operations and Engineering Manager for Electric Regional Operations; Manager of Energy Management Systems; Manager of Operational Technology (OT) Networks; Senior Group Product Manager; and Director of Network infrastructure. I am also a United States Navy veteran and a licensed Professional Engineer in the State of California.

I received a Bachelor of Science degree in Electrical Engineering from San Diego State University and a Master of Science degree in Organizational Leadership from Norwich University. In addition, I hold a Chief Information Security Officer (CISO) certification from Carnegie Mellon University.

I have previously testified before the Commission.

APPENDIX A

GLOSSARY OF TERMS

APPENDIX A

Glossary of Terms

Term	Description
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
BCR	Benefit-Cost Ratio
CA	California
CCPA	California Consumer Privacy Act
CEC	Cybersecurity Engineering and Consulting
CFF	Cross Functional Factor
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CPRA	California Privacy Rights Act
CPUC	California Public Utilities Commission
CSF	Cyber Security Framework
CUI	Controlled Unclassified Information
CWP	Capital Work Paper
DDOS / DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DOE	Department of Energy
DT	Driver/Trigger (RAMP classification)
FERC	Federal Energy Regulatory Commission
FTC Red Flag Rules	Federal Trade Commission Identity-Theft Prevention Regulations
GRC	General Rate Case

Term	Description
IAM	Identity & Access Management
ICS	Industrial Control Systems
IT	Information Technology
LADWP	Los Angeles Department of Water and Power
MFA	Multi-Factor Authentication
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSM	National Security Memorandum
O&M	Operations and Maintenance
OT	Operational Technology
PC	Potential Consequence (RAMP classification)
PKI	Public Key Infrastructure
PMO	Project Management Office
RAMP	Risk Assessment Mitigation Phase
RSE	Risk Spend Efficiency
SA	Security Awareness
SCADA	Supervisory Control and Data Acquisition
SDG&E	San Diego Gas & Electric Company
Sempra	Sempra Energy Corporate Center
SIEM	Security Information and Event Management
SOX	Sarbanes-Oxley Act
SysOps	System Operations (Cyber/IT)
SoCalGas	Southern California Gas Company
SPD	Safety Policy Division
TSA	Transportation Security Administration
TURN	The Utility Reform Network
TVM	Threat & Vulnerability Management
TY	Test Year

Term	Description
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
WAF	Web Application Firewall
XSS	Cross-Site Scripting

APPENDIX B
GLOSSARY OF DEFINITIONS

APPENDIX B

Glossary of Definitions

Appendix B provides definitions of technical terms.

Term	Definition
Advanced Persistent Threat (APT)	A sophisticated threat actor, often associated with nation-states, which gains unauthorized access to systems and maintains long-term presence to conduct espionage or disruption.
Artificial Intelligence (AI)	Refers to technologies used to enhance threat detection and response, and also describes tools used by threat actors to automate attacks and generate deceptive content.
Attack Surface	The total set of digital, physical, and human-facing entry points through which an unauthorized party could attempt to access, disrupt, or extract data from an organization's systems.
Business Continuity	The ability to maintain critical operations and services during and after a cybersecurity incident or disruption.
Cloud-Based Platforms	Systems and applications hosted in cloud environments that support operations, data storage, and system functionality.
Cybersecurity	The protection of information technology and operational technology systems, networks, and data from unauthorized access, disruption, or malicious activity.
Cybersecurity Incident	An event that may disrupt operations, compromise systems, or result in unauthorized access to data or infrastructure.
Cybersecurity Risk	The potential for adverse impacts to safety, reliability, operations, or data resulting from cyber threats, vulnerabilities, or malicious activity.
Cybersecurity Risk Assessment	The evaluation of systems and processes to identify vulnerabilities and determine appropriate mitigation actions.
Deepfake	Artificially generated content used to impersonate individuals or manipulate communications for malicious purposes.
Industrial Control Systems (ICS)	Systems used to monitor and control industrial and utility operations, including energy infrastructure.

Term	Definition
Incident Response	The coordinated activities used to detect, analyze, contain, and remediate cybersecurity incidents.
Internal Defenses	Cybersecurity controls designed to detect, prevent, and respond to threats within internal systems after initial access has occurred.
Malware	Malicious software used to disrupt systems, gain unauthorized access, or damage data.
Multi-vector Threats	Coordinated attacks using various methods to exploit vulnerabilities.
Operational Technology (OT)	Hardware and software used to monitor and control physical processes, including gas and electric system operations.
Perimeter Defenses	Controls that monitor and protect external access points to systems and networks.
Phishing	Deceptive attempts to obtain sensitive information by impersonating trusted entities through electronic communications.
Ransomware	Malicious software that restricts access to systems or data and demands payment for restoration.
Security Operations Center (SOC)	A centralized function responsible for monitoring, detecting, and responding to cybersecurity threats.
Sensitive Data Protection	Controls and processes used to safeguard customer, employee, and company information from unauthorized access or disclosure.
Social Engineering	Techniques used to manipulate individuals into disclosing confidential information or performing actions that compromise security.
Supervisory Control and Data Acquisition (SCADA)	Systems used to monitor and control utility infrastructure operations.
Threat Actor	Individual or group that conducts or attempts to conduct cyberattack against systems or infrastructure.
Threat Intelligence	Information about threats and vulnerabilities used to inform cybersecurity defenses and mitigation strategies.
Vulnerability	Weakness in systems, processes, or controls that may be exploited by a threat actor.
Vulnerability Management	Process of identifying, evaluating, and remediating system weaknesses to reduce cybersecurity risk.

Term	Definition
Zero-Day Exploit	The use of a previously unknown vulnerability to gain unauthorized access or disrupt systems before a mitigation is available.

APPENDIX C
CONTROLS AND MITIGATIONS COMPLIANCE DRIVER ROADMAP

APPENDIX C

Controls and Mitigations Compliance Driver Roadmap

The table below indicates the compliance drivers that underpin Risk Controls/Mitigations identified in testimony. As reflected in this appendix, certain cybersecurity mitigations are driven by specific, prescriptive compliance requirements, while others are prioritized through the Companies' risk-based RAMP process to address evolving threats where formal regulatory standards have not yet been established.

Control/ Mitigation ID	Control/Mitigation Name	Compliance Driver
C801	Perimeter Defenses	NERC Critical Infrastructure Protection (CIP) Standards[73]; TSA Security Directive (SD)
C802	Internal Defenses	NERC CIP Standards; TSA SD
C803	Sensitive Data Protection	NERC CIP Standards; California Consumer Privacy Act (CCPA); TSA SD; Department of Defense's Defense Federal Acquisition Regulation Supplement (DFARS)
C804	Operational Technology (OT) Cybersecurity	NERC CIP Standards; TSA SD
C805	IT Infrastructure Modernization	NERC CIP Standards; TSA SD

[73] NERC CIP Standards are a compliance driver for mitigations presented in this GRC but does not drive the dollars requested in this GRC.

APPENDIX D
CAPITAL EXPENDITURES

San Diego Gas Electric Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity	2026	2027	2028	2029	2030	2031
Total Capital	**-**	**8,690**	**33,818**	**4,661**	**31,457**	**24,935**
2026 - 2028 Capital Request	-	8,690	33,818	-	-	-
Post-Test Year Capital Forecast	-	-	-	4,661	31,457	24,935

San Diego Gas Electric Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity
2026 - 2028 Capital Request

Category	Workpaper Sub	Workpaper Description	In-Service Date	2026	2027	2028
PERIMETER DEFENSES	A09060.001	RAMP - CYBER - SDGE - PERIMETER DEFENSES	11/30/2028	-	-	2,740
	A09060.004	RAMP - CYBER - SDGE - PERIMETER DEFENSES	12/31/2027	-	1,638	-
PERIMETER DEFENSES Total				**-**	**1,638**	**2,740**
INTERNAL DEFENSES	B09060.001	RAMP - CYBER - SDGE - INTERNAL DEFENSES	11/30/2028	-	-	2,740
	B09060.003	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2027	-	936	-
	B09060.004	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2027	-	2,590	-
	B09060.005	RAMP - CYBER - SDGE - INTERNAL DEFENSES	4/30/2028	-	-	5,280
	B09060.007	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2028	-	-	521
	B09060.009	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2028	-	-	903
INTERNAL DEFENSES Total				**-**	**3,526**	**9,444**
SENSITIVE DATA PROTECTION	C09060.001	RAMP - CYBER - SDGE - SENSITIVE DATA PROTECTION	11/30/2028	-	-	4,110
SENSITIVE DATA PROTECTION Total				**-**	**-**	**4,110**
OPERATIONAL TECHNOLOGY CYBERSECURITY	D09060.001	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	4/30/2028	-	-	3,520
	D09060.004	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	787
	D09060.006	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2027	-	936	-
	D09060.007	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	641
	D09060.011	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2027	-	2,590	-
	D09060.012	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	3,145
OPERATIONAL TECHNOLOGY CYBERSECURITY Total				**-**	**3,526**	**8,093**
INFRASTRUCTURE AND PLATFORMS SECURITY LIFE	E09060.003	RAMP - CYBER - SDGE - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	11/30/2028	-	-	2,740
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT Total				**-**	**-**	**2,740**
EMERGING THREAT DEFENSES	F09060.001	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	12/31/2028	-	-	901
	F09060.003	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	12/31/2028	-	-	4,420
	F09060.005	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	11/30/2028	-	-	1,370
EMERGING THREAT DEFENSES Total				**-**	**-**	**6,691**
Grand Total				**-**	**8,690**	**33,818**

San Diego Gas Electric Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity
Post-Test Year Capital Forecast

Category	Workpaper Sub	Workpaper Description	In-Service Date	2026	2027	2028	2029	2030	2031
PERIMETER DEFENSES	A09060.002	RAMP - CYBER - SDGE - PERIMETER DEFENSES	11/30/2030	-	-	-	-	5,280	-
	A09060.003	RAMP - CYBER - SDGE - PERIMETER DEFENSES	4/30/2031	-	-	-	-	-	7,920
	A09060.005	RAMP - CYBER - SDGE - PERIMETER DEFENSES	12/31/2029	-	-	-	813	-	-
PERIMETER DEFENSES Total				**-**	**-**	**-**	**813**	**5,280**	**7,920**
INTERNAL DEFENSES	B09060.002	RAMP - CYBER - SDGE - INTERNAL DEFENSES	11/30/2030	-	-	-	-	5,280	-
	B09060.008	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2031	-	-	-	-	-	252
	B09060.010	RAMP - CYBER - SDGE - INTERNAL DEFENSES	12/31/2031	-	-	-	-	-	1,239
INTERNAL DEFENSES Total				**-**	**-**	**-**	**-**	**5,280**	**1,491**
SENSITIVE DATA PROTECTION	C09060.002	RAMP - CYBER - SDGE - SENSITIVE DATA PROTECTION	11/30/2030	-	-	-	-	7,920	-
SENSITIVE DATA PROTECTION Total				**-**	**-**	**-**	**-**	**7,920**	**-**
OPERATIONAL TECHNOLOGY CYBERSECURITY	D09060.002	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	4/30/2031	-	-	-	-	-	5,280
	D09060.008	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2029	-	-	-	1,003	-	-
	D09060.009	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2030	-	-	-	-	2,027	-
	D09060.010	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2031	-	-	-	-	-	1,269
	D09060.013	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2029	-	-	-	2,845	-	-
	D09060.014	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2030	-	-	-	-	1,945	-
	D09060.015	RAMP - CYBER - SDGE - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2031	-	-	-	-	-	2,600
OPERATIONAL TECHNOLOGY CYBERSECURITY Total				**-**	**-**	**-**	**3,848**	**3,972**	**9,149**
INFRASTRUCTURE AND PLATFORMS SECURITY LIFE	E09060.001	RAMP - CYBER - SDGE - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2030	-	-	-	-	1,085	-
	E09060.002	RAMP - CYBER - SDGE - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2031	-	-	-	-	-	1,086
	E09060.004	RAMP - CYBER - SDGE - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	11/30/2030	-	-	-	-	5,280	-
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT Total				**-**	**-**	**-**	**-**	**6,365**	**1,086**
EMERGING THREAT DEFENSES	F09060.002	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	12/31/2031	-	-	-	-	-	669
	F09060.004	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	12/31/2031	-	-	-	-	-	4,620
	F09060.006	RAMP - CYBER - SDGE - EMERGING THREAT DEFENSES	11/30/2030	-	-	-	-	2,640	-
EMERGING THREAT DEFENSES Total				**-**	**-**	**-**	**-**	**2,640**	**5,289**
Grand Total				**-**	**-**	**-**	**4,661**	**31,457**	**24,935**

Southern California Gas Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity	2026	2027	2028	2029	2030	2031
Total Capital	**49,372**	**51,048**	**103,012**	**65,486**	**88,192**	**121,099**
2026 - 2028 Capital Request	49,372	51,048	103,012	-	-	-
Post-Test Year Capital Forecast	-	-	-	65,486	88,192	121,099

Southern California Gas Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity
2026 - 2028 Capital Request

Category	Workpaper Sub	Workpaper Description	In-Service Date	2026	2027	2028
PERIMETER DEFENSES	A07450.001	RAMP - CYBER - SCG - PERIMETER DEFENSES	3/31/2026	2,765	-	-
	A07450.002	RAMP - CYBER - SCG - PERIMETER DEFENSES	6/30/2026	186	-	-
	A07450.003	RAMP - CYBER - SCG - PERIMETER DEFENSES	6/30/2026	901	-	-
	A07450.004	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2026	553	-	-
	A07450.005	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2026	2,689	-	-
	A07450.006	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2027	-	1,591	-
	A07450.007	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2027	-	7,727	-
	A07450.008	RAMP - CYBER - SCG - PERIMETER DEFENSES	11/30/2028	-	-	3,440
	A07450.009	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2028	-	-	1,088
	A07450.010	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2028	-	-	5,283
PERIMETER DEFENSES Total				**7,094**	**9,318**	**9,811**
INTERNAL DEFENSES	B07450.001	RAMP - CYBER - SCG - INTERNAL DEFENSES	6/30/2026	3,482	-	-
	B07450.002	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2026	3,652	-	-
	B07450.003	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2026	23,039	-	-
	B07450.004	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2027	-	2,230	-
	B07450.005	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2027	-	10,838	-
	B07450.006	RAMP - CYBER - SCG - INTERNAL DEFENSES	4/30/2028	-	-	6,720
	B07450.007	RAMP - CYBER - SCG - INTERNAL DEFENSES	11/30/2028	-	-	3,440
	B07450.008	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2028	-	-	2,139
	B07450.009	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2028	-	-	10,392
INTERNAL DEFENSES Total				**30,173**	**13,068**	**22,691**
SENSITIVE DATA PROTECTION	E07450.001	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2026	969	-	-
	E07450.002	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2026	4,705	-	-
	E07450.003	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2027	-	446	-
	E07450.004	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2027	-	2,168	-
	E07450.005	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	10/31/2028	-	-	35,900
	E07450.006	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	11/30/2028	-	-	5,160
SENSITIVE DATA PROTECTION Total				**5,674**	**2,614**	**41,060**
OPERATIONAL TECHNOLOGY CYBERSECURITY	C07450.001	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	3/31/2026	1,770	-	-
	C07450.002	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2026	102	-	-
	C07450.003	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2026	493	-	-
	C07450.004	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	3/31/2027	-	2,125	-
	C07450.005	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2027	-	851	-
	C07450.006	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2027	-	1,011	-
	C07450.007	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2027	-	6,823	-
	C07450.008	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	4/30/2028	-	-	4,480
	C07450.009	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	789
	C07450.010	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	823
	C07450.011	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2028	-	-	6,891
OPERATIONAL TECHNOLOGY CYBERSECURITY Total				**2,365**	**10,810**	**12,983**
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	007450.001	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	7/31/2026	192	-	-
	007450.002	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	7/31/2026	935	-	-
	007450.003	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	10/31/2026	290	-	-
	007450.004	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	10/31/2026	1,411	-	-
	007450.005	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2027	-	502	-
	007450.006	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2027	-	7,117	-
	007450.007	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	11/30/2028	-	-	3,440
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT Total				**2,828**	**7,619**	**3,440**
EMERGING THREAT DEFENSES	D07450.001	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2026	211	-	-
	D07450.002	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2026	1,027	-	-
	D07450.003	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2027	-	402	-
	D07450.004	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2027	-	7,217	-
	D07450.005	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	11/30/2028	-	-	1,720
	D07450.006	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2028	-	-	1,930
	D07450.007	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2028	-	-	9,377
EMERGING THREAT DEFENSES Total				**1,238**	**7,619**	**13,027**
Grand Total				**49,372**	**51,048**	**103,012**

Southern California Gas Company
Capital Expenditures
(In Thousands of 2025 $)

Cybersecurity
Post-Test Year Capital Forecast

Category	Workpaper Sub	Workpaper Description	In-Service Date	2026	2027	2028	2029	2030	2031
PERIMETER DEFENSES	**A07450.011**	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2029	-	-	-	502	-	-
	A07450.012	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2029	-	-	-	5,865	-	-
	A07450.013	RAMP - CYBER - SCG - PERIMETER DEFENSES	11/30/2030	-	-	-	-	6,720	-
	A07450.014	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2030	-	-	-	-	2,261	-
	A07450.015	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2030	-	-	-	-	16,099	-
	A07450.016	RAMP - CYBER - SCG - PERIMETER DEFENSES	10/31/2031	-	-	-	-	-	40,000
	A07450.017	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2031	-	-	-	-	-	603
	A07450.018	RAMP - CYBER - SCG - PERIMETER DEFENSES	12/31/2031	-	-	-	-	-	5,765
PERIMETER DEFENSES Total				**-**	**-**	**-**	**6,367**	**25,080**	**46,368**
INTERNAL DEFENSES	**B07450.010**	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2029	-	-	-	2,732	-	-
	B07450.011	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2029	-	-	-	22,729	-	-
	B07450.012	RAMP - CYBER - SCG - INTERNAL DEFENSES	7/31/2030	-	-	-	-	825	-
	B07450.013	RAMP - CYBER - SCG - INTERNAL DEFENSES	11/30/2030	-	-	-	-	6,720	-
	B07450.014	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2030	-	-	-	-	1,049	-
	B07450.015	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2030	-	-	-	-	5,100	-
	B07450.016	RAMP - CYBER - SCG - INTERNAL DEFENSES	4/30/2031	-	-	-	-	-	10,080
	B07450.017	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2031	-	-	-	-	-	2,034
	B07450.018	RAMP - CYBER - SCG - INTERNAL DEFENSES	12/31/2031	-	-	-	-	-	25,449
INTERNAL DEFENSES Total				**-**	**-**	**-**	**25,461**	**13,694**	**37,563**
SENSITIVE DATA PROTECTION	**E07450.007**	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2029	-	-	-	1,301	-	-
	E07450.008	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2029	-	-	-	6,322	-	-
	E07450.009	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	11/30/2030	-	-	-	-	10,080	-
	E07450.010	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2030	-	-	-	-	1,152	-
	E07450.011	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2030	-	-	-	-	5,602	-
	E07450.012	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2031	-	-	-	-	-	1,487
	E07450.013	RAMP - CYBER - SCG - SENSITIVE DATA PROTECTION	12/31/2031	-	-	-	-	-	7,225
SENSITIVE DATA PROTECTION Total				**-**	**-**	**-**	**7,623**	**16,834**	**8,712**
OPERATIONAL TECHNOLOGY CYBERSECURITY	**C07450.012**	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2029	-	-	-	812	-	-
	C07450.013	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2029	-	-	-	576	-	-
	C07450.014	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2029	-	-	-	14,651	-	-
	C07450.015	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	3/31/2030	-	-	-	-	3,125	-
	C07450.016	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2030	-	-	-	-	372	-
	C07450.017	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2030	-	-	-	-	1,806	-
	C07450.018	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	4/30/2031	-	-	-	-	-	6,720
	C07450.019	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2031	-	-	-	-	-	1,344
	C07450.020	RAMP - CYBER - SCG - OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY	12/31/2031	-	-	-	-	-	6,533
OPERATIONAL TECHNOLOGY CYBERSECURITY Total				**-**	**-**	**-**	**16,039**	**5,303**	**14,597**
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	**007450.008**	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2029	-	-	-	278	-	-
	007450.009	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2029	-	-	-	1,355	-	-
	007450.010	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	11/30/2030	-	-	-	-	6,720	-
	007450.011	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2030	-	-	-	-	1,087	-
	007450.012	RAMP - CYBER - SCG - INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT	12/31/2031	-	-	-	-	-	1,088
INFRASTRUCTURE AND PLATFORMS SECURITY LIFECYCLE MANAGEMENT Total				**-**	**-**	**-**	**1,633**	**7,807**	**1,088**
EMERGING THREAT DEFENSES	**D07450.008**	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2029	-	-	-	837	-	-
	D07450.009	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2029	-	-	-	7,526	-	-
	D07450.010	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	11/30/2030	-	-	-	-	3,360	-
	D07450.011	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2030	-	-	-	-	1,502	-
	D07450.012	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2030	-	-	-	-	14,612	-
	D07450.013	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2031	-	-	-	-	-	1,005
	D07450.014	RAMP - CYBER - SCG - EMERGING THREAT DEFENSES	12/31/2031	-	-	-	-	-	11,766
EMERGING THREAT DEFENSES Total				**-**	**-**	**-**	**8,363**	**19,474**	**12,771**
Grand Total				**-**	**-**	**-**	**65,486**	**88,192**	**121,099**

APPENDIX E
GRC – RAMP INTEGRATION

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
1CS001.000	NON-SHARED SERVICE CYBERSECURITY - PERIMETER DEFENSES	1OR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	FTEs	85	19	20	19	19	19	19	0	0	0	0	0	0	0
1CS002.000	NON-SHARED SERVICE CYBERSECURITY - INTERNAL DEFENSES	1OR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	FTEs	1,245	1,245	1,245	1,245	1,245	1,245	1,245	0	0	0	0	0	0	0
1CS003.000	NON-SHARED SERVICE CYBERSECURITY - SENSITIVE DATA PROTECTION	1OR08 C803	SDG&E-Risk-8 Cybersecurity Sensitive Data Protection	FTEs	55	57	58	58	58	58	58	0	0	0	0	0	0	0
2100-3101.000	SHARED INTERNAL DEFENSES	1OR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	FTEs	7,062	7,136	7,167	9,977	10,177	10,377	9,976	0	-1	-1	1	1	1	1
2100-3763.000	SHARED PERIMETER DEFENSES	1OR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	FTEs	2,980	3,431	1,736	1,870	1,872	1,874	1,877	9	9	3	4	4	4	4
2100-4128.000	SHARED SENSITIVE DATA PROTECTION	1OR08 C803	SDG&E-Risk-8 Cybersecurity Sensitive Data Protection	FTEs	524	547	550	549	549	549	549	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
2200-0944.000	SHARED SERVICE CYBERSECURITY - INTERNAL DEFENSES	2OR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	FTEs	2,725	2,991	2,716	5,726	5,573	6,073	6,323	0	1	0	0	0	0	0
2200-2491.000	SHARED SERVICE CYBERSECURITY - PERIMETER DEFENSES	2OR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	FTEs	1,475	821	672	767	603	603	603	3	3	3	3	4	4	4
2CS001.000	NON-SHARED SERVICE CYBERSECURITY - PERIMETER DEFENSES	2OR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	FTEs	112	2	2	2	2	2	2	0	0	0	0	0	0	0
2CS002.000	NON-SHARED SERVICE CYBERSECURITY - INTERNAL DEFENSES	2OR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	FTEs	2,286	2,107	1,545	2,341	2,201	2,401	2,201	5	3	3	3	4	4	4

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
A09060.001	A09060.001 - Perimeter Defenses On Premise License	1CR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	2,740	0	0	0	0	0	0	32,000	0	0	0
A09060.002	A09060.002 - Perimeter Defenses On Premise License	1CR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	5,280	0	0	0	0	0	0	32,000	0
A09060.003	A09060.003 - Perimeter Defenses Software	1CR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	0	7,920	0	0	0	0	0	0	32,000
A09060.004	A09060.004 - Perimeter Defenses On Premise Hardware	1CR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	1,638	0	0	0	0	0	0	32,000	0	0	0	0
A09060.005	A09060.005 - Perimeter Defenses On Premise Hardware	1CR08 C801	SDG&E-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	813	0	0	0	0	0	0	32,000	0	0
B09060.001	B09060.001 - Internal Defenses On Premise License	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	2,740	0	0	0	0	0	0	32,000	0	0	0
B09060.002	B09060.002 - Internal Defenses On Premise License	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	5,280	0	0	0	0	0	0	32,000	0
B09060.003	B09060.003 - Internal Defenses	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	936	0	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
B09060.004	B09060.004 - Internal Defenses Software	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	2,590	0	0	0	0	0	0	32,000	0	0	0	0
B09060.005	B09060.005 - Internal Defenses Software	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	5,280	0	0	0	0	0	0	0	0	0	0
B09060.007	B09060.007 - Internal Defenses	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	521	0	0	0	0	0	0	0	0	0	0
B09060.008	B09060.008 - Internal Defenses	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	0	252	0	0	0	0	0	0	0
B09060.009	B09060.009 - Internal Defenses Software	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	903	0	0	0	0	0	0	0	0	0	0
B09060.010	B09060.010 - Internal Defenses Software	1CR08 C802	SDG&E-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	0	1,239	0	0	0	0	0	0	32,000
C09060.001	C09060.001 - Sensitive Data Protection On Premise Software	1CR08 C803	SDG&E-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	4,110	0	0	0	0	0	0	32,000	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
C09060.002	C09060.002 - Sensitive Data Protection On Premise Software	1CR08 C803	SDG&E-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	7,920	0	0	0	0	0	0	32,000	0
D09060.001	D09060.001 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	3,520	0	0	0	0	0	0	32,000	0	0	0
D09060.002	D09060.002 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	5,280	0	0	0	0	0	0	32,000
D09060.004	D09060.004 - Operational Technology (OT) Security On Premise Hardware	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	787	0	0	0	0	0	0	0	0	0	0
D09060.006	D09060.006 - Operational Technology (OT) Security	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	936	0	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
D09060.007	D09060.007 - Operational Technology (OT) Security	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	641	0	0	0	0	0	0	0	0	0	0
D09060.008	D09060.008 - Operational Technology (OT) Security	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	1,003	0	0	0	0	0	0	0	0	0
D09060.009	D09060.009 - Operational Technology (OT) Security	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	2,027	0	0	0	0	0	0	0	0
D09060.010	D09060.010 - Operational Technology (OT) Security	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	1,269	0	0	0	0	0	0	0
D09060.011	D09060.011 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	2,590	0	0	0	0	0	0	32,000	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
D09060.012	D09060.012 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	3,145	0	0	0	0	0	0	0	0	0	0
D09060.013	D09060.013 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	2,845	0	0	0	0	0	0	32,000	0	0
D09060.014	D09060.014 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	1,945	0	0	0	0	0	0	32,000	0
D09060.015	D09060.015 - Operational Technology (OT) Security Software	1CR08 C804	SDG&E-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	2,600	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
E09060.001	E09060.001 - Infrastructure and Platforms Security Lifecycle Management On Premise Hardware	1CR08 C805	SDG&E-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	1,085	0	0	0	0	0	0	32,000	0
E09060.002	E09060.002 - Infrastructure and Platforms Security Lifecycle Management On Premise Hardware	1CR08 C805	SDG&E-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	0	1,086	0	0	0	0	0	0	32,000
E09060.003	E09060.003 - Infrastructure and Platforms Security Lifecycle Management On Premise License	1CR08 C805	SDG&E-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	2,740	0	0	0	0	0	0	32,000	0	0	0
E09060.004	E09060.004 - Infrastructure and Platforms Security Lifecycle Management On Premise License	1CR08 C805	SDG&E-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	5,280	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
F09060.001	F09060.001 - Emerging Threat Defenses	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	901	0	0	0	0	0	0	0	0	0	0
F09060.002	F09060.002 - Emerging Threat Defenses	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	0	669	0	0	0	0	0	0	0
F09060.003	F09060.003 - Emerging Threat Defenses Software	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	4,420	0	0	0	0	0	0	32,000	0	0	0
F09060.004	F09060.004 - Emerging Threat Defenses Software	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	0	4,620	0	0	0	0	0	0	32,000
F09060.005	F09060.005 - Emerging Threat Defenses On Premise License	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	1,370	0	0	0	0	0	0	0	0	0	0
F09060.006	F09060.006 - Emerging Threat Defenses On Premise License	1CR08 M811	SDG&E-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	2,640	0	0	0	0	0	0	32,000	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
007450.001	Infrastructure and Platforms Security Lifecycle Management (Labor)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	192	0	0	0	0	0	0	0	0	0	0	0	0
007450.002	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	935	0	0	0	0	0	0	0	0	0	0	0	0
007450.003	Infrastructure and Platforms Security Lifecycle Management (Labor)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	290	0	0	0	0	0	0	0	0	0	0	0	0
007450.004	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	1,411	0	0	0	0	0	0	32,000	0	0	0	0	0
007450.005	Infrastructure and Platforms Security Lifecycle Management (Labor)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	502	0	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
007450.006	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	7,117	0	0	0	0	0	0	32,000	0	0	0	0
007450.007	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	3,440	0	0	0	0	0	0	32,000	0	0	0
007450.008	Infrastructure and Platforms Security Lifecycle Management (Labor)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	278	0	0	0	0	0	0	0	0	0
007450.009	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	1,355	0	0	0	0	0	0	32,000	0	0
007450.010	Infrastructure and Platforms Security Lifecycle Management (SW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	6,720	0	0	0	0	0	0	32,000	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
007450.011	Infrastructure and Platforms Security Lifecycle Management (Labor & HW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	1,087	0	0	0	0	0	0	0	0
007450.012	Infrastructure and Platforms Security Lifecycle Management (Labor & HW)	2CR08 C805	SCG-Risk-8 Cybersecurity IT Infrastructure Modernization	Users Protected	0	0	0	0	0	0	1,088	0	0	0	0	0	0	32,000
A07450.001	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	2,765	0	0	0	0	0	0	32,000	0	0	0	0	0
A07450.002	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	186	0	0	0	0	0	0	0	0	0	0	0	0
A07450.003	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	901	0	0	0	0	0	0	0	0	0	0	0	0
A07450.004	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	553	0	0	0	0	0	0	0	0	0	0	0	0
A07450.005	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	2,689	0	0	0	0	0	0	0	0	0	0	0	0
A07450.006	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	1,591	0	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
A07450.007	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	7,727	0	0	0	0	0	0	32,000	0	0	0	0
A07450.008	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	3,440	0	0	0	0	0	0	0	0	0	0
A07450.009	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	1,088	0	0	0	0	0	0	0	0	0	0
A07450.010	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	5,283	0	0	0	0	0	0	32,000	0	0	0
A07450.011	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	502	0	0	0	0	0	0	0	0	0
A07450.012	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	5,865	0	0	0	0	0	0	32,000	0	0
A07450.013	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	6,720	0	0	0	0	0	0	0	0
A07450.014	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	2,261	0	0	0	0	0	0	0	0
A07450.015	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	16,099	0	0	0	0	0	0	32,000	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
A07450.016	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	0	40,000	0	0	0	0	0	0	32,000
A07450.017	Perimeter Defenses (Labor)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	0	603	0	0	0	0	0	0	0
A07450.018	Perimeter Defenses (SW)	2CR08 C801	SCG-Risk-8 Cybersecurity Perimeter Defenses	Users Protected	0	0	0	0	0	0	5,765	0	0	0	0	0	0	0
B07450.001	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	3,482	0	0	0	0	0	0	0	0	0	0	0	0
B07450.002	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	3,652	0	0	0	0	0	0	0	0	0	0	0	0
B07450.003	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	23,039	0	0	0	0	0	0	32,000	0	0	0	0	0
B07450.004	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	2,230	0	0	0	0	0	0	0	0	0	0	0
B07450.005	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	10,838	0	0	0	0	0	0	32,000	0	0	0	0
B07450.006	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	6,720	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
B07450.007	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	3,440	0	0	0	0	0	0	0	0	0	0
B07450.008	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	2,139	0	0	0	0	0	0	0	0	0	0
B07450.009	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	10,392	0	0	0	0	0	0	32,000	0	0	0
B07450.010	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	2,732	0	0	0	0	0	0	0	0	0
B07450.011	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	22,729	0	0	0	0	0	0	32,000	0	0
B07450.012	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	825	0	0	0	0	0	0	0	0
B07450.013	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	6,720	0	0	0	0	0	0	32,000	0
B07450.014	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	1,049	0	0	0	0	0	0	0	0
B07450.015	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	5,100	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
B07450.016	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	0	10,080	0	0	0	0	0	0	0
B07450.017	Internal Defenses (Labor)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	0	2,034	0	0	0	0	0	0	0
B07450.018	Internal Defenses (SW)	2CR08 C802	SCG-Risk-8 Cybersecurity Internal Defenses	Users Protected	0	0	0	0	0	0	25,449	0	0	0	0	0	0	32,000
C07450.001	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	1,770	0	0	0	0	0	0	32,000	0	0	0	0	0
C07450.002	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	102	0	0	0	0	0	0	0	0	0	0	0	0
C07450.003	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	493	0	0	0	0	0	0	0	0	0	0	0	0
C07450.004	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	2,125	0	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
C07450.005	Operational Technology Cybersecurity (Labor & HW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	851	0	0	0	0	0	0	0	0	0	0	0
C07450.006	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	1,011	0	0	0	0	0	0	0	0	0	0	0
C07450.007	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	6,823	0	0	0	0	0	0	32,000	0	0	0	0
C07450.008	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	4,480	0	0	0	0	0	0	0	0	0	0
C07450.009	Operational Technology Cybersecurity (Labor & HW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	789	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
C07450.010	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	823	0	0	0	0	0	0	0	0	0	0
C07450.011	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	6,891	0	0	0	0	0	0	32,000	0	0	0
C07450.012	Operational Technology Cybersecurity (Labor & HW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	812	0	0	0	0	0	0	0	0	0
C07450.013	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	576	0	0	0	0	0	0	0	0	0
C07450.014	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	14,651	0	0	0	0	0	0	32,000	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
C07450.015	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	3,125	0	0	0	0	0	0	32,000	0
C07450.016	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	372	0	0	0	0	0	0	0	0
C07450.017	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	1,806	0	0	0	0	0	0	0	0
C07450.018	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	6,720	0	0	0	0	0	0	32,000
C07450.019	Operational Technology Cybersecurity (Labor)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	1,344	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
C07450.020	Operational Technology Cybersecurity (SW)	2CR08 C804	SCG-Risk-8 Cybersecurity Operational Technology (OT) Cybersecurity	Users Protected	0	0	0	0	0	0	6,533	0	0	0	0	0	0	0
D07450.001	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	211	0	0	0	0	0	0	0	0	0	0	0	0
D07450.002	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	1,027	0	0	0	0	0	0	32,000	0	0	0	0	0
D07450.003	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	402	0	0	0	0	0	0	0	0	0	0	0
D07450.004	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	7,217	0	0	0	0	0	0	32,000	0	0	0	0
D07450.005	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	1,720	0	0	0	0	0	0	0	0	0	0
D07450.006	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	1,930	0	0	0	0	0	0	0	0	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
D07450.007	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	9,377	0	0	0	0	0	0	32,000	0	0	0
D07450.008	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	837	0	0	0	0	0	0	0	0	0
D07450.009	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	7,526	0	0	0	0	0	0	32,000	0	0
D07450.010	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	3,360	0	0	0	0	0	0	0	0
D07450.011	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	1,502	0	0	0	0	0	0	0	0
D07450.012	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	14,612	0	0	0	0	0	0	32,000	0
D07450.013	Emerging Threat Defenses (Labor)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	0	1,005	0	0	0	0	0	0	0
D07450.014	Emerging Threat Defenses (SW)	2CR08 M811	SCG-Risk-8 Cybersecurity Emerging Threat Defenses	Users Protected	0	0	0	0	0	0	11,766	0	0	0	0	0	0	32,000

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
E07450.001	Sensitive Data Protection (Labor)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	969	0	0	0	0	0	0	0	0	0	0	0	0
E07450.002	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	4,705	0	0	0	0	0	0	32,000	0	0	0	0	0
E07450.003	Sensitive Data Protection (Labor)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	446	0	0	0	0	0	0	0	0	0	0	0
E07450.004	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	2,168	0	0	0	0	0	0	32,000	0	0	0	0
E07450.005	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	35,900	0	0	0	0	0	0	32,000	0	0	0
E07450.006	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	5,160	0	0	0	0	0	0	0	0	0	0
E07450.007	Sensitive Data Protection (Labor)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	1,301	0	0	0	0	0	0	0	0	0
E07450.008	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	6,322	0	0	0	0	0	0	32,000	0	0

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

Area: CYBERSECURITY

Witness: Omar Zevallos

GRC - RAMP Integration

GRC Workpaper	GRC Wkp Description	RAMP WKP	RAMP Wkp Description	RAMP Unit Measure	TOTAL (in 000s)							UNITS						
					2025	2026	2027	2028	2029	2030	2031	2025	2026	2027	2028	2029	2030	2031
E07450.009	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	10,080	0	0	0	0	0	0	32,000	0
E07450.010	Sensitive Data Protection (Labor)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	1,152	0	0	0	0	0	0	0	0
E07450.011	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	5,602	0	0	0	0	0	0	0	0
E07450.012	Sensitive Data Protection (Labor)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	0	1,487	0	0	0	0	0	0	0
E07450.013	Sensitive Data Protection (SW)	2CR08 C803	SCG-Risk-8 Cybersecurity Sensitive Data Protection	Users Protected	0	0	0	0	0	0	7,225	0	0	0	0	0	0	32,000

Note: Totals may include rounding differences. Total amounts preceded by a double asterisk (**) are in millions ($MM). Unit values preceded by a single asterisk (*) are displayed in thousands (000s).

APPENDIX F
GLOSSARY OF FIGURES

APPENDIX F

Glossary of Figures

Appendix F provides figure consolidation.

Figure Title	Figure Description
Figure OZ-1	Global Average Weekly Cybersecurity Attacks per Organization in Q1
Figure OZ-2	Domestic Cyberattacks in United States between November 2023 and April 2024
Figure OZ-3	Highest Volume Connection Threats Blocked, 2025
Figure OZ-4	Additional Connection Threats Blocked, 2025
Figure OZ-5	Annual Total Companies' Vulnerabilities Remediated vs. Remaining Backlog
Figure OZ-6	Cybersecurity Professionals Outlook on Technology Impacts in 2026

APPENDIX G
GLOSSARY OF TABLES

APPENDIX G

Glossary of Tables

Appendix G provides table consolidation.

Table Title	Table Description
Table OZ-1	Test Year 2028 Summary of Total Costs
Table OZ-2	Non-Shared O&M Summary of Costs
Table OZ-3	Non-Shared O&M Summary of Costs
Table OZ-4	SDG&E Non-Shared O&M Summary of Costs by Workpaper In 2025 Dollars ($000s)
Table OZ-5	SoCalGas Non-Shared O&M Summary of Costs by Workpaper In 2025 Dollars ($000s)
Table OZ-6	San Diego Gas & Electric Company Shared O&M Summary of Costs
Table OZ-7	Southern California Gas Company Shared O&M Summary of Costs
Table OZ-8	SDG&E Shared O&M Summary of Costs by Workpaper In 2025 Dollars ($000s)
Table OZ-9	SoCalGas Shared O&M Summary of Costs by Workpaper In 2025 Dollars ($000s)
Table OZ-10	Southern California Gas Company RAMP and GRC Risk Control/Mitigation Activities - O&M
Table OZ-11	San Diego Gas & Electric Company RAMP and GRC Risk Control/Mitigation Activities - O&M
Table OZ-12	San Diego Gas & Electric Company Capital Expenditures Summary of Costs
Table OZ-13	Southern California Gas Company Capital Expenditures Summary of Costs
Table OZ-14	SDG&E Capital Expenditures Summary of Costs – Perimeter Defenses
Table OZ-15	SoCalGas Capital Expenditures Summary of Costs – Perimeter Defenses
Table OZ-16	SDG&E Capital Expenditures Summary of Costs – Internal Defenses
Table OZ-17	SoCalGas Capital Expenditures Summary of Costs
Table OZ-18	SDG&E Capital Expenditures Summary of Costs – Sensitive Data Protection
Table OZ-19	SoCalGas Capital Expenditures Summary of Costs – Sensitive Data Protection
Table OZ-20	SDG&E Capital Expenditures Summary of Costs – OT
Table OZ-21	SoCalGas Capital Expenditures Summary of Costs – OT
Table OZ-22	SDG&E Capital Expenditures Summary of Costs

Table Title	Table Description
Table OZ-23	SoCalGas Capital Expenditures Summary of Costs
Table OZ-24	SDG&E Capital Expenditures Summary of Costs
Table OZ-25	SoCalGas Capital Expenditures Summary of Costs
Table OZ-26	Southern California Gas Company RAMP and GRC Risk Control/Mitigation Activities – Capital
Table OZ-27	San Diego Gas & Electric Company RAMP and GRC Risk Control/Mitigation Activities - Capital
Table OZ-28	Southern California Gas Company/ San Diego Gas & Electric Company Comparison of RAMP and GRC Risk Control/Mitigation Benefit Cost Ratios