Company: San Diego Gas & Electric Company (U 902 M)
Proceeding: 2024 General Rate Case
Application: A.22-05-___
Exhibit: SDG&E-26

PREPARED DIRECT TESTIMONY OF

LANCE R. MUELLER

(CYBERSECURITY)

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

May 2022

TABLE OF CONTENTS

APPENDICES

SUMMARY

CYBERSECURITY (In 2021 $)			
	2021 Adjusted-Recorded (000s)	**TY2024 Estimated (000s)**	**Change (000s)**
Total Non-Shared Services	19	19	0
Total Shared Services (Incurred)	13,773	16,358	2,585
Total O&M	**13,792**	**16,377**	**2,585**

CYBERSECURITY (In 2021 $)			
Capital	**Estimated 2022 (000s)**	**Estimated 2023 (000s)**	**Estimated 2024 (000s)**
Total CAPITAL	**8,424**	**9,660**	**9,660**

Summary of Requests

Companies currently face constant, ever-changing security threats that continue to increase in complexity, frequency, and sophistication of threat actors. As highlighted through examples discussed in Section I, a cybersecurity incident has the ability to significantly disrupt business operations for the entire enterprise including energy delivery to government agencies, business and residential customers. In order to mitigate these threats, cybersecurity activities are necessary to protect infrastructure, secure customer data, and meet growing privacy regulations. Due to the increased risks and ever-changing tactics used by cybersecurity attackers, a company must remain current in its tools and capabilities, hire skilled people, and develop effective processes and practices for its cybersecurity-related activities. Cybersecurity support services directly contribute to San Diego Gas & Electric Company's (SDG&E) ability to provide secure, safe, and reliable service for customers while maintaining a safe work environment for employees by managing cybersecurity risk. SDG&E's cybersecurity request includes:

- Operations and maintenance (O&M) labor costs to support cybersecurity activities and capital and O&M non-labor costs to implement and maintain technology-based cybersecurity activities.

- Activities to enhance and update cybersecurity infrastructure to minimize the likelihood and impact of ever-changing security threats disrupting business operations and to secure customer data to meet growing privacy regulations.
- Activities that position the Cybersecurity Department to support the continued utilization of technology innovations to enhance the customer experience, increase system capabilities, and gain operational efficiencies by identifying and proactively mitigating cybersecurity risks.

PREPARED DIRECT TESTIMONY OF
LANCE R. MUELLER
(CYBERSECURITY)

I. INTRODUCTION

A. Summary of Cybersecurity Costs and Activities

My testimony supports the Test Year (TY) 2024 forecasts for operations and maintenance (O&M) costs for both non-shared and shared services, and capital costs for the forecast years 2022, 2023, and 2024, associated with the Cybersecurity area for San Diego Gas and Electric Company (SDG&E or Company). SDG&E's forecasted TY 2024 O&M request for Cybersecurity is $16.377 million. The capital request for 2022 is $8.424 million, 2023 is $9.660 million, and 2024 is $9.660 million. Table LM-1 summarizes my sponsored costs.

TABLE LM-1
Test Year 2024 Summary of Total Costs

CYBERSECURITY (In 2021 $)			
	2021 Adjusted-Recorded (000s)	**TY2024 Estimated (000s)**	**Change (000s)**
Total Non-Shared Services	19	19	0
Total Shared Services (Incurred)	13,773	16,358	2,585
Total O&M	**13,792**	**16,377**	**2,585**

CYBERSECURITY (In 2021 $)			
Capital	**Estimated 2022 (000s)**	**Estimated 2023 (000s)**	**Estimated 2024 (000s)**
Total CAPITAL	**8,424**	**9,660**	**9,660**

The Cybersecurity department is responsible for cybersecurity risk management of the information and operational technologies for Southern California Gas Company (SoCalGas), SDG&E, and Sempra Energy Corporate Center (Sempra or Corporate Center) collectively (the Companies). As highlighted in the Information Technology (IT) Policy testimony of Ben Gordon (Exhibit (Ex.) SDG&E-25, Chapter 1), the IT organization is transitioning to a digital focused operating model. Cybersecurity is part of this transition, as mentioned in one of the four key pillars: Proactively Manage Risk through the disciplined management of the lifecycle and cyber risk of infrastructure and applications. The services provided by the Cybersecurity organization are focused on maintaining and improving the Company's security posture in an environment of increasing threat capabilities. Cybersecurity continues to_support technology innovations and enhancements within the business by reducing both the likelihood and potential impact of cybersecurity incidents to all business areas within SoCalGas, SDG&E, and Corporate Center while balancing costs and applying prioritized risk management. Additionally, the department supports enterprise cybersecurity capabilities and provides cybersecurity training and awareness to all users so that they can perform their functions safely, reliably, and securely.

Federal and State agencies (*e.g.*, CPUC, CISA, DHS, FERC, TSA, and DOE)[1] responsible for regulating and setting security standards for companies continue to emphasize the ever-increasing threat level posed by cybersecurity attackers. The evolving regulatory security standards issued by these agencies impact our O&M and Capital forecasts by driving changes in security systems requirements, design, and enhanced security controls and processes. The 2015 and 2016 cybersecurity attacks on the Ukrainian Power Grid and ongoing conflicts highlight the risks and provide insight into how a utility may be impacted by a cybersecurity attack. These cybersecurity attack impacts on the power grid include power system components (*e.g.,* SCADA[2] systems) becoming disabled or maliciously operated by attackers, resulting in potential degradation of safety for Company staff and customers, as well as disruption of power to customers. The attacks on the Ukrainian power systems illustrate how an advanced persistent threat can infiltrate energy delivery management, monitoring, and safety systems.

Also illustrative, another significant cybersecurity incident occurred on May 8, 2021, at Colonial Pipeline.[3] Colonial is one of the largest operators of fuel pipeline in the United States. A ransomware attack shut down its operations, which supplies nearly half of the fuel for the East Coast, and disrupted energy markets and the supply of gas and diesel from the Gulf of Mexico to

[1] California Public Utilities Commission (CPUC), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), Federal Energy Regulatory Commission (FERC), Transportation Security Administration (TSA), Department of Energy (DOE).

[2] Supervisory Control and Data Acquisition (SCADA).

[3] Techtarget.com, 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.

the East Coast. The Colonial cybersecurity incident demonstrates the growing emerging threat to the Companies' critical infrastructure.

Risks associated with unauthorized disclosure of sensitive information also continue to increase. Recent examples include the 2021 FirstEnergy hack in which cyber-thieves attempted to access the accounts of over 6 million customers[4] and the 2022 Washington State Database breach[5] that potentially released sensitive information associated with millions of licensed professionals. The Company's Cybersecurity Program applies lessons learned from these and other events, assessments, and exercises to identify and deploy cyber safety improvements. Additional cybersecurity incidents are shown in Appendix D, Cybersecurity Threat References.

My testimony describes cybersecurity risks, the Cybersecurity Department's approach for managing these risks, and the Cybersecurity Department's activities and costs associated with cybersecurity risk management.

Cybersecurity is a shared service for SDG&E, SoCalGas, and Corporate Center,[6] and the costs set forth in my testimony are allocated between the Companies based on the mechanisms described in the Shared Services Billing, Shared Assets Billing, Segmentation, and Capital Reassignments testimony of Paul Malin and Angel Le (Ex. SCG-30/Ex. SDG&E-34). The cybersecurity risk management activities set forth in my testimony correspondingly benefit SDG&E, SoCalGas, and Corporate Center. The primary drivers for the cybersecurity costs discussed below are for the enhancement or addition of new technical capabilities to address evolving threats and innovative technologies implemented by other business units, replacement of unsupported systems and cybersecurity technology, and the increasing costs to maintain and support cybersecurity technologies.

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

[4] Cleveland.com, FirstEnergy hack is cyber-thieves' latest effort to swipe personal info (September 7, 2021) available at https://www.cleveland.com/business/2021/09/firstenergy-hack-is-cyber-thieves-latest-effort-to-swipe-personal-info.html.

[5] SecurityWeek.com, Breach of Washington State Database May Expose Personal Information, (February 6, 2022) available at https://www.securityweek.com/breach-washington-state-database-may-expose-personal-information.

[6] 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).

- A security policy framework
- Risk management and assessments
- Compliance and vulnerability management
- Cybersecurity awareness and training
- Security assessment
- Business continuity and disaster recovery
- Access Management
- Protective technologies (Network, User, Application)
- System authentication – public key infrastructure (PKI)
- Security Operations Center
    - Monitors security-related activities in systems and applications
    - Anomaly detection
    - Security event detection and escalation
    - Monitors detection infrastructure systems to investigate security events
    - Incident response
    - Exercises/drills

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

B. Support To and From Other Witnesses

My testimony also references the testimony and workpapers of other witnesses, either in support of their testimony or as referential support for mine. Those witnesses are Ben W. Gordon (Ex. SDG&E-25, Ch. 1, Information Technology Policy), R. Scott Pearson (Ex. SCG-03/Ex. SDG&E-03, Ch. 2, RAMP to GRC Integration), and Paul Malin (Ex. SCG-30/Ex. SDG&E-34, Shared Services Billing, Shared Assets Billing, Segmentation, and Capital Reassignments).

C. Organization of Testimony

My testimony is organized as follows:

- Section II provides a summary of SDG&E and SoCalGas's RAMP, defines cybersecurity risk, provides background on the Cybersecurity Program, and discusses the Company's cybersecurity strategy and risk management process.
- Section III discusses SDG&E's sustainability and safety culture.
- Section IV provides the non-shared SDG&E O&M costs.

- Section V provides the shared O&M costs.
- Section VI presents the planned capital categories.
- Section VII concludes with a recap of my requests.
- Section VIII sets forth my witness qualifications.

II. RISK ASSESSMENT MITIGATION PHASE (RAMP) INTEGRATION

Certain costs supported in my testimony are driven by activities described in SDG&E's and SoCalGas' respective 2021 Risk Assessment Mitigation Phase (RAMP) Reports (the 2021 RAMP Reports).[7] The 2021 RAMP Reports presented an assessment of the key safety risks for SDG&E and SoCalGas and proposed plans for mitigating those risks. As discussed in the testimony of the RAMP to GRC Integration witnesses R. Scott Pearson and Gregory S. Flores (Ex. SCG-03/SDG&E-03, Chapter 2), the costs of risk mitigation projects and programs were translated from the 2021 RAMP Reports into the individual witness areas.

In the course of preparing the Cybersecurity General Rate Case (GRC) forecasts, SDG&E continued to evaluate the scope, schedule, resource requirements, changes to the threat landscape, and synergies of RAMP-related projects and programs. Therefore, the final presentation of RAMP costs may differ from the ranges shown in the 2021 RAMP Reports. Table LM-2 and Table LM-3 provide summaries of the RAMP-related costs supported in my testimony.

TABLE LM-2
Summary of RAMP O&M Costs

CYBERSECURITY Summary of RAMP O&M Costs (In 2021 $)			
	BY2021 Embedded Base Costs (000s)	**TY2024 Estimated Total (000s)**	**TY2024 Estimated Incremental (000s)**
RAMP Risk Chapter			
SDG&E-Risk-6 Cybersecurity	13,792	16,377	2,585
Sub-total	13,792	16,377	2,585
Total RAMP O&M Costs	**13,791**	**16,376**	**2,585**

[7] *See* Application (A.) 21-05-011/-014 (cons.) (RAMP Proceeding). Please refer to the RAMP to GRC Integration testimony of R. Scott Pearson and Gregory S. Flores (Ex. SCG-03/SDG&E-03, Chapter 2) for more details regarding the 2021 RAMP Reports.

TABLE LM-3
Summary of RAMP Capital Costs

CYBERSECURITY Summary of RAMP Capital Costs (In 2021 $)				
	2022 Estimated RAMP Total (000s)	**2023 Estimated RAMP Total (000s)**	**2024 Estimated RAMP Total (000s)**	**2022-2024 Estimated RAMP Total (000s)**
RAMP Risk Chapter				
SDG&E-Risk-6 Cybersecurity	8,424	9,660	9,660	27,744
Sub-total	8,424	9,660	9,660	27,744
Total RAMP Capital Costs	**8,424**	**9,660**	**9,660**	**27,744**

A. RAMP Risk Overview

As summarized in Table LM-2 and Table LM-3 above, my testimony includes costs to mitigate the safety-related risks included in the RAMP report.[8] These risks are further described in Table LM-4 below:

TABLE LM-4
RAMP Risk Chapter Description

SDG&E-Risk-6 – Cybersecurity	The risk of a cybersecurity incident to gas and electric control systems, all company data and information systems, operational technology (OT)[9] systems, and related processes.

In developing my request, priority was given to these key safety risks to assess which risk mitigation activities Cybersecurity currently performs and what incremental efforts are needed to further mitigate these risks. While developing the GRC forecasts, SDG&E evaluated the scope, schedule, resource requirement, changes to the threat landscape, and synergies of RAMP-related projects and programs to determine costs already covered in the base year and those that are incremental increases expected in the test year. The Cybersecurity Program, described in detail below, continually reassesses current mitigation activities versus best practices and threats created by continually evolving threat actor capabilities and increasing use of innovative

[8] Unless otherwise indicated, references to the 2021 RAMP Report refers to SDG&E's RAMP Report.

[9] Operational technology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.

technologies within the business. In addition to safety risks, the Cybersecurity Program addresses other risk area impacts such as operations, compliance, and financial with cybersecurity risk management activities. Cybersecurity risk mitigations are designed to address as many business services and systems as possible. Activities discussed in this testimony support RAMP.

Messrs. Pearson and Flores (Ex. SCG-03/SDG&E-03, Chapter 2) discuss all of the risks and Cross Functional Factors (CFFs) included in the 2021 RAMP Reports and the RAMP to GRC integration process.

1. Cybersecurity Risk

Cybersecurity risk involves a major cybersecurity incident that causes disruptions to electric or gas operations (*e.g.*, SCADA system) or results in damage or disruption to company operations, reputation, or disclosure of sensitive data, and loss of customer data.

Electric and gas operations, safety systems, information processing, and other utility functions are highly reliant on technology, automation, and integration with other systems. The complex interoperation of these systems and the rapid changes that occur in the industry in response to climate, cost, and other drivers create a risk situation where inadvertent actions or maliciously motivated events can potentially disrupt core operations or disclose sensitive data, among other serious consequences.

In the previous RAMP and GRC filing, the Cybersecurity mitigation plan was structured using the National Institute of Standards and Technology (NIST) Cyber Security Framework to group like security controls. In the 2021 RAMP and this Test Year (TY) 2024 GRC, the Companies are using operational groups to describe, and group mitigations in a more business-aligned approach.

2. Operational Groups

The cyber activity areas discussed throughout my testimony focus on activities performed or supported directly by the Cybersecurity department as a shared service for SDG&E, SoCalGas, and Corporate Center. The Cybersecurity department manages cybersecurity risks across the enterprise. This department is made up of the following groups: Cybersecurity Policy & Risk Management; Cybersecurity Program Office; IT Service Continuity Management; Monitoring Response & System Operations; IT Compliance Enablement; Cybersecurity Engineering and Consulting (CEC); Threat & Vulnerability Management (TVM); and Security Awareness (SA).

The Cybersecurity program utilizes risk management frameworks, including but not limited to the NIST Cyber Security Framework, Center for Internet Security (CIS-20), NIST 800-53, and MITRE ATT&CK framework. Additionally, the Companies comply with applicable laws and regulations both at the State and Federal level.

The Companies have considered the evolving threat and regulatory landscape of cybersecurity risk in the design of our planned activities. The Companies have adopted a structure of five comprehensive activity areas that balance risk mitigation and cost effectiveness while also establishing foundational security capabilities that will serve to mitigate risks from evolving threats. The planned activities are designed to provide adequate risk reduction to offset the projected Cybersecurity risk increase to maintain this risk at a manageable level.

These five activity areas include:

- Perimeter Defenses
- Internal Defenses
- Sensitive Data Protection
- Operational Technology (OT) Cybersecurity
- Obsolete Information Technology (IT) Infrastructure and Application Replacement

My testimony includes the costs to support and maintain these five areas. The details of these activity areas are explained in Section VI.

B. GRC Risk Controls and Mitigations

Table LM-5 below provides a narrative summary of the forecasted RAMP-related activities that I sponsor in my testimony.

TABLE LM-5
Summary of RAMP Risk Activities

RAMP ID	Activity	Description
SDG&E-Risk-6-C01	Perimeter Defenses	The Perimeter Defenses program includes activities that protect the external access points of the Company's internal IT systems. Perimeter Defenses are designed to prevent cybersecurity attacks, detect unauthorized access, and protect the integrity of IT systems.
SDG&E-Risk-6-C02	Internal Defenses	The Internal Defenses program activities are designed to detect and prevent unauthorized users, those misusing authorized credentials and malicious software (*i.e.*, malware) from propagating inside of

RAMP ID	Activity	Description
		the perimeter, moving within the IT system or into the Operational Technology (OT) system.
SDG&E-Risk-6-C03	Sensitive Data Protection	The Sensitive Data Protection projects enhance technology to reduce the risk of unauthorized access to customer and Company information.
SDG&E-Risk-6-C04	Operational Technology Cybersecurity	The OT Cybersecurity program focuses on securing the electric and gas control systems for the Companies.
SDG&E-Risk-6-C05	Obsolete IT Infrastructure and Application Replacement	The Obsolete IT Infrastructure and Application Replacement program activities refresh technology at regular intervals to minimize security risks posed by obsolete technologies.

These activities are discussed further below in Section VI, as well as in my workpapers. For additional information and a roadmap, please refer to Appendix B and C, which contain tables identifying by workpaper the TY 2024 forecast dollars associated with activities in the 2021 RAMP Report that are discussed in this testimony.

The RAMP risk mitigation efforts are associated with specific actions, such as programs, projects, processes, and utilization of technology. For each of these mitigation efforts, an evaluation was made to determine the portion, if any, that was already performed as part of historical activities (*i.e.*, embedded base costs) and the portion, if any, that was incremental to base year activities. Furthermore, for the incremental activities, a review was completed to determine if any portion of incremental activity was part of the workgroup's base forecast methodology. The result is what SDG&E considers to be a true representation of incremental increases over the base year.

My incremental request supports the ongoing management of these risks that could pose significant safety, reliability, and financial consequences. The anticipated risk reduction benefits that may be achieved by the incremental request set forth in my testimony are all associated with reducing cybersecurity risk.

C. Changes from RAMP Report

As discussed in more detail in the RAMP to GRC Integration testimony of Messrs. Pearson and Flores (Ex. SCG-03/SDG&E-03, Chapter 2), in the RAMP Proceeding, the Commission's Safety Policy Division (SPD) and intervenors provided feedback on the

Companies' 2021 RAMP Reports. Appendix B in Ex. SCG-03/SDG&E-03, Chapter 2 provides a complete list of the feedback and recommendations received and the Companies' responses.

General changes to risks scores or Risk Spend Efficiency (RSE) values are primarily due to changes in the Multi-Attribute Value Framework (MAVF) and RSE methodology, as discussed in the RAMP to GRC Integration testimony. Other than these changes, the RAMP-related activities described in my GRC testimony are consistent with the activities presented in the 2021 RAMP Report. Changes from the 2021 RAMP Report presented in my testimony, including updates to forecasts, are summarized as follows:

- The forecast dollars in the 2021 RAMP Report are provided on a post-allocation basis and the dollars in my testimony are forecast on a total incurred basis.

III. SUSTAINABILITY AND SAFETY CULTURE

Sustainability, safety and reliability are the cornerstones of SDG&E's core business operations and are central to SDG&E's GRC presentation. SDG&E is committed to not only deliver clean, safe, and reliable electric and natural gas service, but to do so in a manner that supports California's climate policy, adaptation, and mitigation efforts. In support of the legal and regulatory framework set by the state, SDG&E has set a goal to reach Net Zero greenhouse gas (GHG) emissions by 2045, adopted a Sustainability Strategy to facilitate the integration of GHG emission reduction strategies into SDG&E's day-to-day operations and long-term planning, and published an economy-wide GHG Study that recommends a diverse approach for California leveraging clean electricity, clean fuels, and carbon removal to achieve the 2045 goals through the lens of reliability, affordability, and equity. The Sustainability Strategy serves as SDG&E's guide to enable a more just and equitable energy future in SDG&E's service territory and beyond. As a "living" strategy, SDG&E will continue to update the goals and objectives as technologies, policies, and stakeholder preferences change. *See* the Sustainability Policy testimony of Estela de Llanos (Ex. SDG&E-02).

In this GRC, SDG&E focuses on three major categories that underpin the Sustainability Strategy: mitigating climate change, adapting to climate change, and transforming the grid to be the reliable and resilient catalyst for clean energy. SDG&E's goal is to contribute to the decarbonization of the economy by way of diversifying energy resources, collaborating with regional partners, and providing customer choice that enables an affordable, flexible, and resilient grid.

Safety is a core value and SDG&E is committed to providing safe and reliable service to all its stakeholders. This safety-first culture is embedded in every aspect of the Company's work. In 2020, SDG&E commenced development and deployment of a Safety Management System (SMS), which better aligns and integrates safety, risk, asset, and emergency management across the entire organization. Cybersecurity supports the enterprise SMS initiative by maintaining the security of the Company's network communication infrastructure and the integrity of the information exchanged in SMS. More broadly, Cybersecurity supports the broader safety and security goals of protecting the availability and reliability of the electric grid and gas distribution critical infrastructure for the Company, its customers, and the public.

SDG&E remains focused on identifying and implementing the most cost-effective solutions with the potential to make the greatest impact on reducing GHG emissions, while maintaining a safe and reliable energy system. SDG&E believes that safety, reliability, and sustainability are inextricably linked and fundamental to the Company's ability to continue to successfully operate. Please see the Sustainability Policy testimony of Estela de Llanos (Ex. SDG&E-02) for additional detail on SDG&E's Sustainability Strategy and the Safety, Risk and Asset Management Systems testimony of Kenneth J. Deremer (Ex. SDG&E-31) for additional detail on SDG&E's Safety Policy.

The Cybersecurity Program is dedicated to cybersecurity aspects of providing safe and reliable energy delivery while protecting customer information and ensuring compliance with regulations. Cybersecurity efforts toward achieving a safety culture include the identification of risks, the assignment of specific roles and responsibilities, remediating identified risks and vulnerabilities, tracking cybersecurity threats, providing cybersecurity awareness and training, participating in government, industry, and community information sharing activities, and providing incident response capabilities to mitigate those risks.

Finally, part of SDG&E's commitment to safety is the continuous implementation of safety training and education of SDG&E's workforce for securely using technology. Well-trained technology users are effective cybersecurity risk mitigations for social engineering attacks such as phishing. The Cybersecurity Program's focus on awareness and outreach is designed to provide safety, security-oriented training, and communication to all Company employees through many activities and programs to improve their cybersecurity behaviors at work and at home. These activities and programs include outreach across the business, providing tools to share cybersecurity-related information and answer questions, and training in multiple forms, including mandatory cybersecurity training.

IV. NON-SHARED COSTS

"Non-Shared Services" are activities that are performed by a utility solely for its own benefit. Table LM-7 summarizes the total non-shared O&M forecasts for the listed cost categories.

TABLE LM-7
Non-Shared O&M Summary of Costs

CYBERSECURITY **(In 2021 $)**			
Categories of Management	**2021 Adjusted-Recorded (000s)**	**TY2024 Estimated (000s)**	**Change (000s)**
A. Cybersecurity	19	19	0
Total Non-Shared Services	**19**	**19**	**0**

A. Non-Shared Cybersecurity

1. Description of Costs and Underlying Activities

These non-shared SDG&E cybersecurity costs represent non-labor for the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity team. The amount represented in the table above are for non-FERC activities that support the day-to-day operations of the NERC CIP team.

This cost category includes the support costs associated with the protection of electric grid transmission infrastructure that falls under regulatory compliance with NERC CIP requirements.

a. RAMP Activities

RAMP-related costs for non-shared cybersecurity include the costs for the following activities: (1) Perimeter Defenses, (2) Internal Defenses, (3) Sensitive Data Protection, (4) Operational Technology Cybersecurity, and (5) Obsolete IT Infrastructure and Application Replacement. These activities are described in Table LM-5 above.

Table LM-8 below provides the RAMP activities, their respective cost forecasts, and the RSEs for this workpaper. For additional details on these RAMP activities, please refer to my workpapers Ex. SDG&E-26-WP 1CS001.000.

TABLE LM-8
RAMP Activity O&M Forecasts by Workpaper
In 2021 Dollars ($000)

Workpaper	RAMP ID	Activity	2021 Embedded -Recorded	TY 2024 Estimated	Change	GRC RSE*
1CS001.000	SDG&E -Risk-6 – C01-C05	All Mitigations	$19	$ 19	$0	-

* *See* Capital workpapers Ex. SDG&E-26-CWP for mitigation level RSE[10] values, which contain both O&M and Capital and shared and non-shared dollars and benefits.

2. Forecast Method

The forecast methodology developed for this cost category is the base year (2021) recorded, plus adjustments. 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. An evolving threat landscape, cybersecurity attacker sophistication, and threat complexity requires us to use current data and adjustments rather than relying on historical averages that do not account for increased defenses needed to combat these growing cybersecurity threats.

3. Cost Drivers

The cost drivers behind this forecast include the continuing need to address increasing exposure to cybersecurity risk to the energy sector business and its customers. Recent research and analytics indicate a cybersecurity risk growth rate of up to 27% year over year.[11] Additionally, new and current Federal and State regulations requiring the implementation of specific cybersecurity practices has increased our cybersecurity program needs. One example of a new cybersecurity regulation is the 2021 Transportation Security Administration (TSA)

[10] SDG&E believes it has identified an error during the finalization of this testimony after the point at which it could be corrected prior to filing. The corresponding RSE calculation will be revised at another available opportunity.

[11] Ponemon Institute and Accenture, 2017 Cost of Cyber Crime Study, Insights on the Security Investments That Make a Difference (2017) at 4, (according to 2017 statistics, there are over 130 large-scale, targeted breaches in the U.S. per year, and that number is growing by 27 percent per year), available at https://www.accenture.com/_acnmedia/pdf-62/accenture-2017costcybercrime-us-final.pdf#zoom=50.

Security Directive Pipeline-2021-02.[12] To mitigate this evolving risk and comply with the numerous regulatory mandates pertaining to cybersecurity,[13] increased O&M costs are necessary to cover labor and non-labor necessary to maintain prior investments, as well as for additional headcount to implement, support, operate and manage improvements made through capital projects.

V. SHARED COSTS

As described in the testimony of Paul Malin (Ex. SCG-30/Ex. SDG&E-34), Shared Services are activities performed by a utility shared services department (*i.e.*, functional area) for the benefit of: (i) SDG&E or SoCalGas, (ii) 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.

I am sponsoring the forecasts 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. SDG&E-34-WP. The dollar amounts allocated to affiliates are presented in our Shared Services Policy and Procedures testimony. *See* Shared Services Billing, Shared Assets Billing, Segmentation, and Capital Reassignments testimony of Paul Malin and Angel Le (Ex. SCG-30/Ex. SDG&E-34).

Table LM-9 summarizes the total shared O&M forecasts for the listed cost categories.

TABLE LM-9
Shared O&M Summary of Costs

CYBERSECURITY (In 2021 $)			
(In 2021 $) Incurred Costs (100% Level)			
Categories of Management	**2021 Adjusted-Recorded (000s)**	**TY2024 Estimated (000s)**	**Change (000s)**
A. Cybersecurity	13,773	16,358	2,585
Total Shared Services (Incurred)	**13,773**	**16,358**	**2,585**

[12] Federal Register.gov, Ratification of Security Directive (September 24, 2021) available at https://www.federalregister.gov/documents/2021/09/24/2021-20738/ratification-of-security-directive.

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

A. Shared Cybersecurity

1. Description of Costs and Underlying Activities

At the Companies, cybersecurity is critical to the safe and reliable delivery of electric and gas service to our customers, including critical infrastructure providers in our Southern California service territory (*e.g.*, financial services, telecommunication providers, other utilities). Our service territory includes millions of people, one of the nation's busiest ports, some of the largest cities in California, most critical military bases, countless defense contractors and small businesses.

Cybersecurity is a unique risk, as compared to other risks driven by operations and asset management, because it deals with intelligent adversaries that are attempting to achieve their objectives by gaining access to Company systems or information through artifice or other improper means.

Cybersecurity threats have continued to evolve, increase, and become more complex and impactful year over year. Adversaries continue to use an evolving and increasingly more sophisticated set of tools and strategies to conduct attacks on the energy sector. Their suite of capabilities includes advanced malware, complex phishing attacks, identification of non-public vulnerabilities, ransomware, among others.

The criticality of cybersecurity is evidenced 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. They 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). The recent cybersecurity attacks on Ukraine by Russia provides but one example of this increasing threat landscape. This current situation has led the CISA and other agencies to issue numerous threat advisories describing the Russian government's malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries. These advisories reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing.[14] Additionally, Microsoft recently released a report[15] warning that it saw six Russia-aligned, state-sponsored hacking groups launch over 237 cybersecurity attacks against Ukraine starting in the weeks before Russia's February 24, 2022 invasion. According to the report, "More than 40% of the destructive attacks were aimed at organizations in critical infrastructure sectors that could have negative second-order effects on the government, military, economy, and people."[16] The Companies believe their cybersecurity forecast is prudent and reasonable to address the existing and growing threat.

The shared Cybersecurity costs represent labor and non-labor for the Cybersecurity area where costs are shared among multiple business units and support the Company goals of safety, reliability, and maintenance. The Cybersecurity O&M forecasts include the resources and systems maintenance needs for the functional groups mentioned above in Section II.A.2, "Operational Groups" and described below:

- Cybersecurity Risk Management & Governance
  - The Cybersecurity Risk Management and Governance group facilitates the ongoing process of identifying, analyzing, evaluating, and addressing Company cybersecurity risks. Primary responsibilities include the evaluation and treatment of risks, gathering and reporting of risk metrics, managing cybersecurity Policy & Standards, and coordinating cybersecurity assessments.
- Cybersecurity Program Office:
  - The Cybersecurity Program Office is responsible for alignment and prioritization of projects to achieve the strategic Cybersecurity objectives and ensure the successful execution and production deployment of new capabilities.
- IT Service Continuity Management (ITSCM)

[14] CISA, Russia Cyber Threat Overview and Advisories, available at https://www.cisa.gov/uscert/russia.

[15] Microsoft, Digital Security Unit, Special Report: Ukraine, An overview of Russia's cyberattack activity in Ukraine (April 27, 2022), available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[16] *Id.* at 4.

  - The ITSCM team's role is to minimize the effects of outages and disruptions on business operations. ITSCM's practices enable the Companies to reduce impact to operations after problems occur, reduce the risk of data loss and reputational harm, and improve operations while decreasing the chance of emergencies. ITSCM provides governance around standards and compliance over disaster recovery (DR) and business continuity (BC) processes.

- Monitoring Response & System Operations
  - The Monitoring Response and System Operations groups include the Security Operations Center (SOC), Incident Response, Insider Threat, and Cyber Threat Intelligence groups. Combined these groups serve as the focal point for cyber incident management through 24/7 monitoring, alerting and detection, proactive threat hunting, intelligence driven defense and digital behavioral analysis to defend and/or respond to cybersecurity attacks, suspicious activity and mitigate potential harm or risk to the Company.

- IT Compliance Enablement
  - The IT Compliance Enablement team is responsible for facilitating compliance with laws, rules, regulations, and internal Company standards pertaining to IT and Cybersecurity. This team also assists and coordinates the assessment of technology-related compliance issues across the organization.

- Cybersecurity Engineering and Consulting (CEC)
  - The primary role of the CEC group is to provide cybersecurity expertise to business projects and efforts. Additionally, they perform security assessments of systems, applications, and the security programs of vendors and other third parties.

- Threat & Vulnerability Management (TVM)
  - The TVM group is responsible for the identification, evaluation, prioritization, and reporting of security vulnerabilities in systems and the software that runs on them by using a risk-based approach to drive

vulnerability remediation of threats and minimizing their impact to the Companies.

- Security Awareness (SA)
  - o The SA group's main responsibility is to educate all employees, staff and contractors to be sure they know, understand, and follow the Company’s security requirements and behave in a secure manner. SA training and awareness programs are designed to help users and employees understand the role they play in helping to prevent cybersecurity incidents.

a. RAMP Activities

RAMP-related costs for non-shared cybersecurity include the costs for the following activities: (1) Perimeter Defenses, (2) Internal Defenses, (3) Sensitive Data Protection, (4) Operational Technology Cybersecurity, and (5) Obsolete IT Infrastructure and Application Replacement. These activities are described in Table LM-5 above.

Table LM-10 below provides the RAMP activities, their respective cost forecasts, and the RSEs for this workpaper. For additional details on these RAMP activities, please refer to my workpapers Ex. SDG&E-26-WP 2100-3101.000.

TABLE LM-10
RAMP Activity O&M Forecasts by Workpaper
In 2021 Dollars ($000)

Workpaper	RAMP ID	Activity	2021 Embedded -Recorded	TY 2024 Estimated	Change	GRC RSE*
2100-3101.000	SDG&E-Risk-6 – C01-C05	All Mitigations	$13,773	16,358	$2,585	-

* *See* Capital workpapers for mitigation level RSE values, which contain both O&M and Capital and shared and non-shared dollars and benefits.

2. Forecast Method

The forecast methodology developed for this cost category is the base year (2021) recorded, plus adjustments. 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. An evolving threat landscape, cybersecurity attacker sophistication, and threat complexity requires us to use current data and adjustments rather than relying on historical averages that do not account for increased defenses needed to combat these growing cybersecurity threats.

3. Cost Drivers

The cost drivers behind this forecast include the continuing need to address increasing exposure to cybersecurity risk to the energy sector business and its customers. Recent research and analytics indicate a cybersecurity risk growth rate of up to 27% year over year.[17] Additionally, new and current Federal and State regulations requiring the implementation of specific cybersecurity practices has increased our cybersecurity program needs. One example of a new cybersecurity regulation is the 2021 Transportation Security Administration (TSA) Security Directive Pipeline-2021-02.[18] To mitigate this evolving risk and comply with the numerous regulatory mandates pertaining to cybersecurity,[19] increased O&M costs are necessary to cover labor and non-labor costs necessary to maintain prior investments, as well as for additional headcount to implement, support, operate and manage improvements made through capital projects.

VI. CAPITAL

A. Introduction

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, and 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 best practices, and striving to keep pace with changing threats.

Historical activities will continue to be performed. However, due to the evolving nature of the threats associated with this risk, if only current activities were to be maintained, the risk would likely grow. Accordingly, the Companies are looking to new activities and technologies to improve or replace existing security capabilities to address the ever-changing threats and/or supported technologies. While it is possible to plan for technology refresh costs based on the

[17] *See, supra*, n.10.

[18] *See, supra,* n.11.

[19] *See, supra*, n.12.

useful lifetime of a solution, it is more difficult to predict reactive technology costs 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. A side effect of the risk management adjustments is that planned activities are continually reprioritized and restructured. For example, activities defined beyond a 12- to 18-month planning horizon are less likely to be implemented and may be replaced by a higher priority activity. Also, activities may happen in different years due to changes in priority and resource availability as a result of the continuous reassessment of threats, known risks, and prioritization. Table LM-11 summarizes the total capital forecasts for 2022, 2023, and 2024.

TABLE LM-11
Capital Expenditures Summary of Costs

CYBERSECURITY (In 2021 $)			
A. Cybersecurity	**Estimated 2022(000s)**	**Estimated 2023(000s)**	**Estimated 2024(000s)**
1. Perimeter Defenses	0	2,300	2,300
2. Internal Defenses	1,138	1,150	1,150
3. Sensitive Data Protection	995	1,610	1,610
4. Operational Technology (OT) Cybersecurity	6,291	3,450	3,450
5. Obsolete Information Technology (IT) Infrastructure and Application Replacement	0	1,150	1,150
Total	**8,424**	**9,660**	**9,660**

B. Capital Forecast Methodologies

SDG&E Cybersecurity capital projects use a zero-based forecast methodology. A zero-based estimate is a more accurate indicator of future costs for this forecast category based on current and expected projects of this nature as there is no regular historical average for reference. Detailed cost estimates are provided by internal and external personnel (where applicable) experienced in estimating projects with similar scope, schedule, and resources. SDG&E continues to invest in Cybersecurity technology resources (labor and non-labor) that are based on current market quotes and industry conditions.

C. Capital Cost Drivers

Cybersecurity's capital categories are risk mitigation activities driven by the evolving and increasingly more sophisticated tools and strategies threat actors use to conduct attacks on the energy sector. These activities are designed to enhance our perimeter defenses, internal defenses sensitive data protection, operational technology (OT)[20] cybersecurity, and obsolete IT infrastructure and applications replacement. Cybersecurity's 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.

D. Perimeter Defenses

1. Description of Costs and Underlying Activities

The forecast for Perimeter Defenses for 2022, 2023, and 2024 are $0, $2.300 million, and $2.300 million, respectively. SDG&E plans to build and place in service Perimeter Defenses by the Test Year. 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 our perimeter.

[20] *See, supra*, n.9.

Perimeter Defenses reduce the frequency or probability of successful attacks. As a security strategy, it accomplishes this by limiting access to authorized users, reducing the likelihood that malicious code will enter the information technology environment, and delaying or frustrating potential cybersecurity attackers. This strategy also helps the Companies to understand the number of pathways into or out of the perimeter while simultaneously monitoring the perimeter in real time.

The types of perimeter defense projects presented in this activity area include efforts such as firewall upgrades and process automation, web application firewall protections, distributed denial of service (DDoS) protection, and the implementation of other perimeter defensive and threat mitigation mechanisms.

Information regarding Perimeter Defense is found in the capital workpapers. *See* Ex. SDG&E-26-CWP 00906G.000 – Perimeter Defenses. Perimeter Defenses mitigate safety risks identified in the 2021 RAMP Report: Risk–6 Cybersecurity – C01 Perimeter Defenses. Accordingly, this forecast in its entirety aligns with a RAMP activity.

For Perimeter Defenses, Table LM-12 below shows the TY 2024 forecast dollars and RSE associated with the activities in the 2021 RAMP Report.

TABLE LM-12
RAMP Activity Capital Forecasts by Workpaper
In 2021 Dollars ($000s)

Workpaper	**Risk Chapter**	**ID**	**Description**	**2022 Estimated RAMP Total**	**2023 Estimated RAMP Total**	**2024 Estimated RAMP Total**	**GRC RSE***
00906G.001	SDG&E-Risk-6	C01	Perimeter Defenses	$ 0	$ 2,300	$ 2,300	497

* The RSE value includes O&M and Capital dollars.

E. Internal Defenses

1. Description

The forecast for Internal Defenses for 2022, 2023, and 2024 are $1.138 million, $1.150 million, and $1.150 million, respectively. SDG&E plans 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 (*i.e.*, malware) from propagating inside of the perimeter, moving within the IT system or into the OT system. The enhancements to the Companies' IT and OT systems' Access Management system reduces 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 reduce the risk to internal assets and 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, which improves the ability to identify and respond to threats more quickly. The enhancements to the IT and OT systems' Access Management system allow the Companies to keep the current risk level steady.

Use of "browser based" and Virtual Desktop Infrastructure (VDI) further helps improve the effectiveness of Internal Defense activities. VDI is defined as the hosting of desktop environments on a central server. It is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and are delivered to end clients over a network. This IT strategy reduces the cybersecurity attackers' threat surface by limiting their ability to compromise and establish a foothold on any one device or endpoint and then pivot to other resources on the network.

The types of internal defense activities include efforts such as more effective endpoint security monitoring, enhancements in threat and vulnerability management, incident management, third party and supply chain risk mitigation, and cloud security.

Information regarding Internal Defenses is found in the capital workpapers. *See* Ex. SDG&E-26-CWP 00906H.001 – Internal Defenses. Internal Defenses mitigates safety risks identified in the 2021 RAMP Report: Risk–6 Cybersecurity – C02 Internal Defenses. Accordingly, this forecast in its entirety aligns with a RAMP activity.

For Internal Defenses, Table LM-13 below shows the TY 2024 forecast dollars and RSE associated with the activities in the 2021 RAMP Report.

TABLE LM-13
RAMP Activity Capital Forecasts by Workpaper
In 2021 Dollars ($000s)

Workpaper	Risk Chapter	ID	Description	2022 Estimated RAMP Total	2023 Estimated RAMP Total	2024 Estimated RAMP Total	GRC RSE*
00906H.001	SDG&E-Risk-6	C02	Internal Defenses	$ 1,138	$ 1,150	$ 1,150	295

* The RSE value includes O&M and Capital dollars.

F. Sensitive Data Protection

1. Description

The forecast for Sensitive Data Protection for 2022, 2023, and 2024 are $0.995 million, $1.610 million, and $1.610 million, respectively. SDG&E plans 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. The Sensitive Data Protection activity area helps reduce the risk of unauthorized access to the Companies' information 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. The activities for this area will help the Companies continue the prudent management of sensitive data. The Companies' current activities target sensitive data within information technology systems, including laptops and other mobile computing devices.

The types of sensitive data activities include efforts such as Identity Access Management (IAM) enhancements, Data Loss Prevention (DLP), mobile device security and data crawler technology to identify sensitive data in the environment.

Information regarding Sensitive Data Protection is found in the capital workpapers. See Ex. SDG&E-26-CWP 00906K.001 – Sensitive Data Protection. Sensitive Data Protection mitigates safety risks identified in the 2021 RAMP Report: Risk–6 Cybersecurity – C03 Sensitive Data Protection. Accordingly, this forecast in its entirety aligns with a RAMP activity.

For the Sensitive Data Protection, Table LM-14 below shows the TY 2024 forecast dollars and RSE associated with the activities in the 2021 RAMP Report.

TABLE LM-14
RAMP Activity Capital Forecasts by Workpaper
In 2021 Dollars ($000s)

Workpaper	Risk Chapter	ID	Description	2022 Estimated RAMP Total	2023 Estimated RAMP Total	2024 Estimated RAMP Total	GRC RSE*
00906K.001	SDG&E-Risk-6	C03	Sensitive Data Protection	$ 995	$ 1,610	$ 1,610	199

* The RSE value includes O&M and Capital dollars.

G. Operational Technology (OT) Cybersecurity

1. Description

The forecast for OT Cybersecurity for 2022, 2023, and 2024 are $6.291 million, $3.450 million, and $3.450 million, respectively. SDG&E plans to build and place in service OT Cybersecurity by the Test Year. The OT Cybersecurity program focuses on securing the electric and gas control systems for the Companies. OT environments enable critical business functions, including safe and reliable energy delivery to customers throughout the service territory. OT Cybersecurity requires a specialized approach in order to balance operational needs with cybersecurity risk. Improving asset management helps identify unauthorized systems, which could potentially be a source of an attack. Network anomaly detection, endpoint detection, and security event monitoring improve visibility into 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 maintain a secure OT system and mitigate the increasing potential threat on that critical system.

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 communication infrastructure. 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[21] and SCADA) such as ensuring proper network segmentation, multifactor authentication, network anomaly detection, advanced security information and event management (SIEM) and analytics, environment network access control, environment endpoint detection response, malware defense and more secure remote connection capabilities.

Information regarding OT Cybersecurity is found in the capital workpapers. *See* Ex. SDG&E-26-CWP 00906I.001 –OT Cybersecurity. OT Cybersecurity mitigates safety risks identified in the 2021 RAMP Report: Risk–6 Cybersecurity – C04 OT Cybersecurity. Accordingly, this forecast in its entirety aligns with a RAMP activity.

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

For the OT Cybersecurity, Table LM-15 below shows the TY 2024 forecast dollars and RSE associated with the activities in the 2021 RAMP Report.

TABLE LM-15
RAMP Activity Capital Forecasts by Workpaper
In 2021 Dollars ($000s)

Workpaper	Risk Chapter	ID	Description	2022 Estimated RAMP Total	2023 Estimated RAMP Total	2024 Estimated RAMP Total	GRC RSE*
00906I.001	SDG&E-Risk-6	C04	Operational Technology (OT) Cybersecurity	$ 6,291	$ 3,450	$ 3,450	520

* The RSE value includes O&M and Capital dollars.

H. Obsolete IT Infrastructure and Application Replacement

1. Description

"Obsolete IT Infrastructure and Applications" refers to systems that have fallen out of manufacturer support and could have a cybersecurity impact. Systems no longer supported by their manufacturer can pose a cybersecurity risk because, for example, security patches and updates are no longer provided.

The forecast for Obsolete IT Infrastructure and Application Replacement for 2022, 2023, and 2024 are $0, $1.150 million, and $1.150 million, respectively. SDG&E plans to build and place in service Obsolete IT Infrastructure and Application Replacement activities by the Test Year. One of the fundamental practices that supports a strong cybersecurity program is the refresh of technology, both hardware and software, at regular intervals, to minimize risks posed by technologies that are no longer supported by vendors and lead to security risks. This is frequently referred to as "Foundational Technology Systems Lifecycle Management." The cybersecurity specific activities in this activity area include tools and processes to identify and remediate cybersecurity risks from obsolete systems.

Technology lifecycles are short and require frequent upgrades to meet modern security standards and capabilities. In addition to technology obsolescence, this approach also addresses security obsolescence. Security obsolescence refers to cybersecurity tools and processes that are no longer effective, or potentially could 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 types of Obsolete IT Infrastructure and Application Replacement activities include technology refreshes and/or replacements of infrastructure, operating systems, middleware, and applications. Additionally, there is the need to provide ongoing system maintenance activity to confirm continued secure configurations, patching, and upgrading, among others. Lastly, the need to utilize effective architecture and other mechanisms to confirm high availability and service continuity for critical systems.

Information regarding Obsolete IT Infrastructure and Application Replacement is found in the capital workpapers. See Ex. SDG&E-26-CWP 00906J.001 – Obsolete IT Infrastructure and Application Replacement. Obsolete IT Infrastructure and Application Replacement mitigates safety risks identified in the 2021 RAMP Report: Risk–6 Cybersecurity – C05 Obsolete IT Infrastructure and Application Replacement. Accordingly, this forecast in its entirety aligns with a RAMP activity.

For the Obsolete IT Infrastructure and Application Replacement, Table LM-16 below shows the TY 2024 forecast dollars and RSE associated with the activities in the 2021 RAMP Report.

TABLE LM-16
RAMP Activity Capital Forecasts by Workpaper
In 2021 Dollars ($000s)

Workpaper	Risk Chapter	ID	Description	2022 Estimated RAMP Total	2023 Estimated RAMP Total	2024 Estimated RAMP Total	GRC RSE*
00906J.001	SDG&E-Risk-6	C05	Obsolete IT Infrastructure and Application Replacement	$ 0	$ 1,150	$ 1,150	366

* The RSE value includes O&M and Capital dollars.

VII. CONCLUSION

These forecasts are expected to allow SDG&E to continue to maintain its current security posture in an environment of evolving threat agent capabilities and increasing adoption of innovative technology.

This concludes my prepared direct testimony.

VIII. WITNESS QUALIFICATIONS

My name is Lance Mueller. My primary work location is 488 8th Ave, San Diego, CA. 92101. I am currently employed by SDG&E as the Director of Cybersecurity, Risk and Compliance. In this role, I oversee all Cybersecurity services provided across SDG&E, SoCalGas and Corporate Center.

Previously my positions have included Cybersecurity Director and Cybersecurity Manager at Sempra Energy. Prior to joining Sempra Energy, I held similar positions with several corporate organizations and spent 15 years in law enforcement, where I was assigned to investigate cybercrime. I hold an active national security clearance at the secret level.

I have a Bachelor of Science in Cybersecurity and Information Assurance and I am completing a Master of Science degree in Cybersecurity Operations and Leadership. I am a graduate of the Carnegie Mellon Executive Chief Information Security Officer (CISO) course and I hold several cyber risk management professional certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and several technical certifications.

I have not previously testified before the Commission.

APPENDIX A

Glossary of Terms

APPENDIX A – Glossary of Terms

Term	**Description**
CFF	Cross Functional Factor
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CPUC	California Public Utilities Commission
CSF	Cyber Security Framework
CWP	Capital Work Paper
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DOE	Department of Energy
FERC	Federal Energy Regulatory Commission
GRC	General Rate Case
IAM	Identity Access Management
ICS	Industrial Control Systems
IT	Information Technology
MAVF	Multi-Attribute Value Framework
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OT	Operational Technology
PKI	Public Key Infrastructure
RAMP	Risk Assessment Mitigation Phase
RSE	Risk Spend Efficiency
SCADA	Supervisory Control and Data Acquisition
SoCalGas	Southern California Gas Company

SDG&E	San Diego Gas & Electric Company
SIEM	Security Information and Event Management
SPD	Safety Policy Division
TSA	Transportation Security Administration
TVM	Threat and Vulnerability Management
TY	Test Year
VDI	Virtual Desktop Infrastructure
VM	Virtual Machines
WAF	Web Application Firewalls
XXS	Cross-Site Scripting

APPENDIX B

Summary of Safety Related Risk Mitigation Costs by Workpaper – O&M

APPENDIX B - Summary of Safety Related Risk Mitigation Costs by Workpaper – O&M

CYBERSECURITY RAMP Activity O&M Forecasts by Workpaper (In 2021 $)						
Workpaper	**RAMP ID**	**Description**	**BY2021 Embedded Base Costs (000s)**	**TY2024 Estimated Total (000s)**	**TY2024 Estimated Increment al (000s)**	**GRC RSE***
1CS001.000	SDG&E-Risk-6 - C01 - C05	All Mitigations	19	19	0	-
2100-3101.000	SDG&E-Risk-6 - C01 - C05	All Mitigations	13,772	16,357	2,585	-
Total			**13,791**	**16,376**	**2,585**	**-**

* *See* Capital workpapers Ex. SDG&E-26-CWP for mitigation level RSE[22] values, which contain both O&M and Capital and shared and non-shared dollars and benefits.

[22] SDG&E believes it has identified an error during the finalization of this testimony after the point at which it could be corrected prior to filing. The corresponding RSE calculation will be revised at another available opportunity.

APPENDIX C

Summary of Safety Related Risk Mitigation Costs by Workpaper – Capital

APPENDIX C - Summary of Safety Related Risk Mitigation Costs by Workpaper – Capital

CYBERSECURITY RAMP Activity Capital Forecasts by Workpaper (In 2021 $)						
Workpaper	**RAMP ID**	**Description**	**2022 Estimated RAMP Total (000s)**	**2023 Estimated RAMP Total (000s)**	**2024 Estimated RAMP Total (000s)**	**GRC RSE***
00906G.001	SDG&E-Risk-6 - C01	Perimeter Defenses	0	2,300	2,300	497
00906H.001	SDG&E-Risk-6 - C02	Internal Defenses	1,138	1,150	1,150	295
00906I.001	SDG&E-Risk-6 - C04	Operational Technology (OT) Cybersecurity	6,291	3,450	3,450	520
00906J.001	SDG&E-Risk-6 - C05	Obsolete Information Technology (IT) Infrastructure and Application Replacement	0	1,150	1,150	366
00906K.001	SDG&E-Risk-6 - C03	Sensitive Data Protection	995	1,610	1,610	199
Total			**8,424**	**9,660**	**9,660**	**-**

* The RSE value includes O&M and Capital dollars.

APPENDIX D

Cybersecurity Threat References

APPENDIX D – Cybersecurity Threat References

A representative sample of recent threats facing the energy industry is provided below:

OT Attacks on Utility Infrastructure

Title: Ukrainian power grid 'lucky' to withstand Russian cyber-attack
Link: https://www.bbc.com/news/technology-61085480
Summary: 04/12/22: The Ukrainian government has revealed it narrowly averted a serious cybersecurity attack on the country's power grid. Hackers targeted one of its largest energy companies, trying to shut down sub-stations, which would have caused blackouts for two million people. The malicious software used in the attack is similar to that used by Russian hackers who previous caused power cuts in Kyiv. Researchers believe Russian military group Sandworm is responsible. It is the most serious cybersecurity attack so far launched against Ukraine since the Russian invasion.

Title: Colonial Pipeline hack explained: Everything you need to know
Link: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
Summary: 04/26/22: The Colonial Pipeline was the victim of a ransomware attack in May 2021. It infected some of the pipeline's digital systems, shutting it down for several days. The shutdown affected consumers and airlines along the East Coast. The hack was deemed a national security threat, as the pipeline moves oil from refineries to industry markets. The Colonial Pipeline is one of the largest and most vital oil pipelines in the U.S.

Title: Hackers try to contaminate Florida town's water supply through computer breach
Link: https://www.reuters.com/article/us-usa-cyber-florida/hackers-try-to-contaminate-florida-towns-water-supply-through-computer-breach-idUSKBN2A82FV
Summary: 02/08/21: Hackers remotely accessed the computer system of a facility that treats water for about 15,000 people near Tampa, Florida, and sought to add a dangerous level of additive to the water supply. This breach illustrates the connection between cybersecurity and the potential consequence of serious injury/harm.

Title: Energy company EDP confirms cyberattack, Ragnar Locker ransomware blamed

Link: https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/

Summary: 07/07/2020: EDP Renewables North America (EDPR NA) disclosed a cybersecurity attack in which ransomware infected parent company Energias de Portugal's (EDP) systems, potentially leading to information exposure. The energy firm denied the loss of customer data. Cybersecurity attackers claim to have stolen ten terabytes of business records.

Title: U.S. Government Issues Powerful Cyberattack Warning as Gas Pipeline Forced into Two Day Shut Down

Link: https://www.forbes.com/sites/kateoflahertyuk/2020/02/19/us-government-issues-powerful-cyberattack-warning-as-gas-pipeline-forced-into-two-day-shut-down/?sh=3dcb3d8d5a95

Summary: 02/19/20: A major cybersecurity attack targeted a gas compression facility, forcing it to shut it down for two days as it struggled to recover, according to an alert from the U.S. government.

Title: 'Denial of service' attack caused grid cyber disruption: DOE

Link: https://www.eenews.net/stories/1060254751

Summary: 03/05/2019: A recent cyber disruption to the US grid involved a "denial of service condition" at a Western utility.

Title: Cyber-Attack Against Ukrainian Critical Infrastructure

Link: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

Summary: 02/25/2016: This was a well-publicized and understood attack by a nation-state on the electrical transmission system in Ukraine. This was an advanced attack that migrated from the IT to OT system and resulted in the loss of electric load to approximately 200,000 customers.

Insider Attacks

Title: Arizona Waste Water Worker Charged with Terrorism

Link: https://www.officer.com/home/news/10251659/ariz-waste-water-worker-charged-with-terrorism

Summary: 04/02/2011: A City of Mesa Water Resources employee was charged with terrorism and making terrorist threats after he turned off numerous wastewater treatment operating systems at a facility overnight.

Title: Capital One former insider

Link: https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

Summary: 07/29/2019: An insider, formerly employed by Amazon Web Services (AWS), illicitly penetrated vulnerabilities in the AWS configurations to enable access to the Capital One customer data.

Supply Chain

Title: A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

Link: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Summary: 04/16/2021: SolarWinds, a major U.S. information technology firm, was the subject of a cybersecurity attack that spread to its clients and went undetected for months. Foreign hackers, who some top U.S. officials believe are from Russia, were able to use the hack to spy on private companies like the elite cybersecurity firm FireEye and the upper echelons of the U.S. Government, including the Department of Homeland Security and Treasury Department.

Title: Major hack of US agencies may have started with software company SolarWinds

Link: https://www.cnet.com/news/major-hack-of-us-agencies-may-have-started-with-software-company-solarwinds/

Summary: 12/15/2020. In a filing with the Securities and Exchange Commission, SolarWinds said the vulnerable Orion updates were delivered to customers between March and June, and as many as 18,000 customers may have downloaded the software.

Title: America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

Link: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

Summary: 01/10/2019: Reports that a Russian group accessed an electric utility via one of the utility's smaller vendors. The Companies are monitoring a growing concern in cyber with respect to harmful vulnerabilities introduced in the supply chain.

IT Cybersecurity

Title: Hackers are using DDoS attacks to squeeze victims for ransom

Link: https://www.techradar.com/news/hackers-are-using-ddos-attacks-to-squeeze-victims-for-ransom

Summary: 01/09/21: A major Fortune Global 500 company was targeted by a Ransom DDoS (RDDoS) attack in late 2020. This extortion attempt was part of a wider trend of ransom campaigns that unfolded throughout last year. Cybercriminals will likely continue to use similar methods as they have been quite successful.

Title: An Old Bot's Nasty New Tricks: Exploring Qbot's Latest Attack Methods

Link: https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

Summary: 08/27/20. An Electricity Information Sharing and Analysis Center (E-ISAC) partner shared a report of Qakbot malware and Cobalt Strike tools beaconing in their environment. The E-ISAC has tracked similar activity that use Qakbot and Cobalt Strike for installation of malicious payloads, including ProLock ransomware, against multiple organizations in the United States. Open-source investigation of the indicators convey a fixed association with either Qakbot phishing email or command and control activity using Cobalt Strike.

Title: ThreatConnect Research Roundup: Spoofing SharePoint

Link: https://threatconnect.com/blog/threatconnect-research-roundup-spoofing-sharepoint/

Summary: In April 2020, a government partner report identified the registration of a lookalike domain of a U.S.-based energy engineering company by unknown threat actors. The company being imitated, HPI Energy Services Ltd., specializes in turbine and utility plant control systems integration. According to the report, the threat actors created a primary and two sub-domains that host fake Microsoft SharePoint-themed login pages for a probable credential harvesting campaign. These fake sites are likely aimed at collecting credentials of HPI Energy Services employees.