Risk Assessment and Mitigation Phase

(Chapter SCG/SDG&E-Risk-6)

Cybersecurity

May 17, 2021

TABLE OF CONTENTS

RISK: CYBERSECURITY

I. INTRODUCTION

The purpose of this chapter is to present Southern California Gas Company's (SoCalGas) and San Diego Gas & Electric Company's (SDG&E) (collectively, the Companies) risk mitigation plan for the Cybersecurity risk. This risk chapter is identical for both Companies given that Cybersecurity risk is currently managed centrally for both Companies. Each chapter in this Risk Assessment Mitigation Phase (RAMP) Report contains the information and analysis that meets the requirements adopted in Decision (D.) 16-08-018 and D.18-12-014 and the Settlement Agreement included therein at Attachment A (the Settlement Decision).[1]

SoCalGas and SDG&E have identified and defined RAMP risks in accordance with the process described in further detail in Chapter RAMP-B of this RAMP Report. On an annual basis, SoCalGas' and SDG&E's Enterprise Risk Management (ERM) organizations facilitate the Enterprise Risk Registry (ERR) process. The ERR process influenced how risks were selected for inclusion in this 2021 RAMP Report, consistent with the Settlement Decision's directives, as discussed in Chapter RAMP-C.

The RAMP Report's purpose is to present a current assessment of key safety risks and the proposed activities for mitigating those risks. The RAMP Report does not request funding. Any funding requests will be made in SoCalGas' and SDG&E's General Rate Case (GRC) application. The costs presented in this 2021 RAMP Report are those costs for which SoCalGas and SDG&E anticipate requesting recovery in its Test Year (TY) 2024 GRC. SoCalGas' and SDG&E's TY 2024 GRC presentation will integrate developed and updated funding requests from the 2021 RAMP Report, supported by witness testimony.[2] This 2021 RAMP Report is presented consistent with SoCalGas' and SDG&E's GRC presentation, in that the last year of recorded data (2020) provides baseline costs and cost estimates are provided for years 2022-

[1] D.16-08-018 adopted the requirements previously set forth in D.14-12-025. D.18-12-014, the Phase Two Decision Adopting Safety Model Assessment Proceeding (S-MAP) Settlement Agreement With Modifications, adopted the Settlement Agreement Among Pacific Gas and Electric Company, Southern California Edison Company, Southern California Gas Company, San Diego Gas & Electric Company, The Utility Reform Network, Energy Producers and Users Coalition, Indicated Shippers, and the Office of Ratepayer Advocates, which contains the minimum required elements to be used by the utilities for risk and mitigation analysis in the RAMP and General Rate Case.

[2] *See* D.18-12-014 at Attachment A, A-14 ("Mitigation Strategy Presentation in the RAMP and GRC").

2024, as further discussed in Chapter RAMP-A. This 2021 RAMP Report presents capital costs as a sum of the years 2022, 2023, and 2024 as a three-year total; operations and maintenance (O&M) costs are only presented for TY 2024 (consistent with the GRC). Costs for each activity that directly address each risk are provided where those costs are available and within the scope of the analysis required in this RAMP Report.

Throughout this 2021 RAMP Report, activities are delineated between controls and mitigations, consistent with the definitions adopted in the Settlement Decision's Revised Lexicon. A "control" is defined as a "[c]urrently established measure that is modifying risk."[3] A "mitigation" is defined as a "[m]easure or activity proposed or in process designed to reduce the impact/consequences and/or likelihood/probability of an event."[4] Activities presented in this chapter are representative of those that are primarily scoped to address SoCalGas' and SDG&E's Cybersecurity risk; however, many of the activities presented herein also help mitigate other areas.

As discussed in Chapters RAMP-A and RAMP-C, SoCalGas and SDG&E have endeavored to calculate a Risk Spend Efficiency (RSE) for all controls and mitigations presented in this risk chapter. However, for controls and mitigations where no meaningful data or Subject Matter Expert (SME) opinion exists to calculate the RSE, SoCalGas and SDG&E have included an explanation why no RSE can be provided, in accordance with California Public Utilities Commission (CPUC or Commission) Safety Policy Division (SPD) staff guidance.[5] Activities with no RSE value presented in this 2021 RAMP Report (if any) are identified in Section V below.

A. Risk Overview

At the Companies, cybersecurity is critical to the safe and reliable delivery of electric and gas service to customers, including critical infrastructure providers in Southern California (*e.g.*, financial services, telecommunication providers, other utilities). The Companies' service

[3] *Id*. at 16.

[4] *Id.* at 17.

[5] *See* Safety Policy Division Staff Evaluation Report on PG&E's 2020 Risk Assessment and Mitigation Phase (RAMP) Application (A.) 20-06-012 (November 25, 2020) at 5 ("SPD recommends PG&E and all IOUs provide RSE calculations for controls and mitigations or provide an explanation for why it is not able to provide such calculations.").

territories include millions of people, one of the nation's busiest ports, some of country's largest cities, 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. In addition, gaining information about the Companies' security controls and mitigation plans could be useful to an adversary – and not only directly harm the Companies, but also indirectly harm the Companies' stakeholders. Cybersecurity threats have continued to increase and have become more complex and impactful year over year. For these reasons, publishing the Companies' cybersecurity-related controls, intelligence, strategies, and tactics in the public record could aid those adversaries, the bad actors that are attempting to disrupt the Companies' systems and society at large. Sensitive details associated with the content of this Chapter are available upon Commission request for discussion in person.

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, that are targeting critical infrastructure for economic exploit, espionage, or covert action in preparation for some overt act (*e.g.*, disrupting energy supply). The Companies believe their investment and spend in cybersecurity is prudent and reasonable to address the existing and growing threat.

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, and ransomware, among others. A current example of increased threat complexity and impact is the recent SolarWinds breach.[6] This breach was so significant in breadth and depth that the effect and impact, as of this writing, are still being investigated and understood. The United States (US) Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC) were two of many entities affected by this breach. In fact, a directive by the Cybersecurity and

[6] *See* E&E News, Cybersecurity, *'This is bad.' Hacking chaos engulfs FERC, DOE, Microsoft* (December 18, 2020), *available at* https://www.eenews.net/stories/1063721065.

Infrastructure Security Agency (CISA) and a "North American Electric Reliability Corporation (NERC) Alert- Essential Action" have been issued for this breach.[7]

Most recently, another significant cybersecurity incident occurred on May 8, 2021 at Colonial Pipeline. Colonial is the operator of the largest fuels pipeline in the US. This cybersecurity ransomware attack affected its information technology (IT) and operations technology (OT) systems, requiring Colonial Pipeline to shut down operations. The Colonial cybersecurity incident further illustrates the growing emerging threat to the Companies' critical infrastructure, given the trends cited below:

- Cyberattacks targeting critical infrastructure or key companies, some by suspected foreign actors, have become a growing area of concern for the US national security officials.[8]
- "Cybersecurity analysts say companies have been targeted with ransomware for several years, and that the attacks are becoming more brazen and costly, particularly since the start of the pandemic."[9]
- "As companies shifted to remote work, fewer employees worked exclusively within protected networks, creating more opportunities for hackers to break into their systems, cybersecurity analysts say."[10]
- According to Homeland Security Secretary Alejandro Mayorkas, "The rate of ransomware attacks increased 300% in 2020."[11]

Energy regulators have also recognized the threat cyberattacks pose to the energy sector. In a recent Notice of Proposed Rulemaking (NOPR), FERC notes that the energy sector "faces numerous and complex cybersecurity challenges at a time of both great change in the operation of the transmission system and an increase in the number and nature of attack methods." The NOPR also recognizes that "[t]hese ever-expanding risks create challenges in defending the

[7] NERC has responsibility for oversight of the Bulk Power System and to provide guidance and insight such as via alerts like this. *See* Cybersecurity & Infrastructure Security Agency, Alert (AA20-352A), *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (revised April 15, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[8] *See, e.g.*, Collin Eaton and Dustin Volz, *U.S Pipeline Cyberattack Forces Closure*, The Wall St. Journal (WSJ), May 8, 2021; James Rundle and David Uberti, *How Can Companies Cope with Ransomware*, WSJ, May 9, 2021. *See also*, Collin Eaton, *Pipeline's Shutdown Exposes Cyber Threat to Power Sector*, WSJ, May 10, 2021.

[9] James Rundle and David Uberti, *How Can Companies Cope with Ransomware*, WSJ, May 9, 2021.

[10] *Id.*

[11] *Id.*

digitally interconnected components of the grid from cyber exploitation."[12] This acknowledgment has been underscored by the realization of various threats. For example, in 2016, a Ukrainian utility experienced an OT attack on utility infrastructure that resulted in the loss of electric load to approximately 200,000 customers.[13] Cybersecurity-related attacks were also experienced in 2019 and 2020 on other gas and electric operators that caused unforeseen disruptions to business operations.[14]

Given that the Companies' cybersecurity threats continue to evolve rapidly, the Companies' strategy to counter cybersecurity threats must be flexible and enable adaption to these evolving threats over time. Accordingly, timely and accurate Cybersecurity Threat Intelligence (CTI) is key to staying abreast of this ever-changing threat landscape. SoCalGas and SDG&E rely on Federal, State, and Local government partnerships for intelligence feeds along with peer utility industry relationships and private (subscription) based services for Industrial Control Systems (ICS) cybersecurity threat intelligence. The Companies also obtain cybersecurity threat intelligence from a variety of entities and sources, including Information Sharing and Analysis Centers (ISACs), the Federal Bureau of Investigations (FBI), FERC, the DOE, the Department of Homeland Security (DHS), CISA, Transportation Security Administration (TSA) and a variety of US intelligence community agencies. Information from threat intelligence sources in the utility industry continues to reveal adversaries that are using advanced tradecraft in their attempts to access our nation's utility systems.

[12] Federal Energy Regulatory Commission, *FERC Proposes Incentives for Cybersecurity Investments by Public Utilities* (December 17, 2020), *available at https://www.ferc.gov/news-events/news/ferc-proposes-incentives-cybersecurity-investments-public-utilities*.

[13] *See* Cybersecurity & Infrastructure Security Agency, ICS Alert (IR-ALERT-H-16-056-01) *Cyber-Attack Against Ukrainian Critical Infrastructure* (revised August 23, 2018), *available at https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.*

[14] *See* Kate O'Flaherty, *U.S. Government Issues Powerful Cyberattack Warning As Gas Pipeline Forced Into Two Day Shut Down*, Forbes, February 19, 2020, *available at 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.*

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

OT Attacks on Utility Infrastructure

Title: Ransomware Attack Shuts Down Biggest U.S. Gasoline Pipeline

Link: *https://www.bloomberg.com/news/articles/2021-05-08/u-s-s-biggest-gasoline-and-pipeline-halted-after-cyberattack*

Summary: 05/08/21: The operator of the biggest gasoline pipeline in the US shut down operations late Friday following a cybersecurity attack that has threatened to roil energy markets and upend the supply of gas and diesel to the East Coast. Colonial is a key artery for the eastern half of the US. It is the main source of gasoline, diesel, and jet fuel for the East Coast, with a capacity of about 2.5 million barrels a day on its system from Houston to as far as North Carolina and another 900,000 barrels a day to New York.

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 cyberattack 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. 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 cyberattack 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 US 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: Attack on Ukrainian Electric Operator

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 Utility Worker Charged

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: SolarWinds Breach

Link: *https://www.businessinsider.com/solarwinds-hack-explained-governmentagencies-cyber-security-2020-12*

Summary: 12/24/2020: SolarWinds, a major US information technology firm, was the subject of a cyberattack that spread to its clients and went undetected for months. Foreign hackers, who some top US 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 US 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: Russian attack on electric utility suppliers

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 US-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.

B. Risk Definition

For purposes of this RAMP Application, the Companies' Cybersecurity risk is defined as the risk of a major cybersecurity incident, which results in disruptions to electric or gas operations (*e.g.*, Industrial Control Systems, supply, transmission, distribution, storage) and/or damage or disruption to the Companies' operations, reputation, or disclosure of sensitive customer or Company data.

C. Scope

Table 1 below provides what is considered in scope for the Cybersecurity risk in this RAMP Application.

Table 1: Risk Scope

In-Scope:	The scope of this risk includes gas and electric control systems, all company data and information systems, operational technology systems, and related processes.
Data Quantification Sources:	SoCalGas & SDG&E engaged internal data sources for the calculation surrounding risk reduction; however, if data was insufficient, industry or national data was supplemented and adjusted to fit the risk profile associated with the operating locations and perimeter of the utilities. For example, certain types of incident events have not occurred within the SoCalGas & SDG&E service territories; therefore, expanding the quantitative needs to encompass industry data where said incident(s) have been recorded provides a proxy and is justified in establishing a baseline of risk and risk addressed by activities.

Additional information on data quantification sources for the Cybersecurity risk, the potential gas system impacts, and electric system impacts is provided in Appendix B.

II. RISK ASSESSMENT

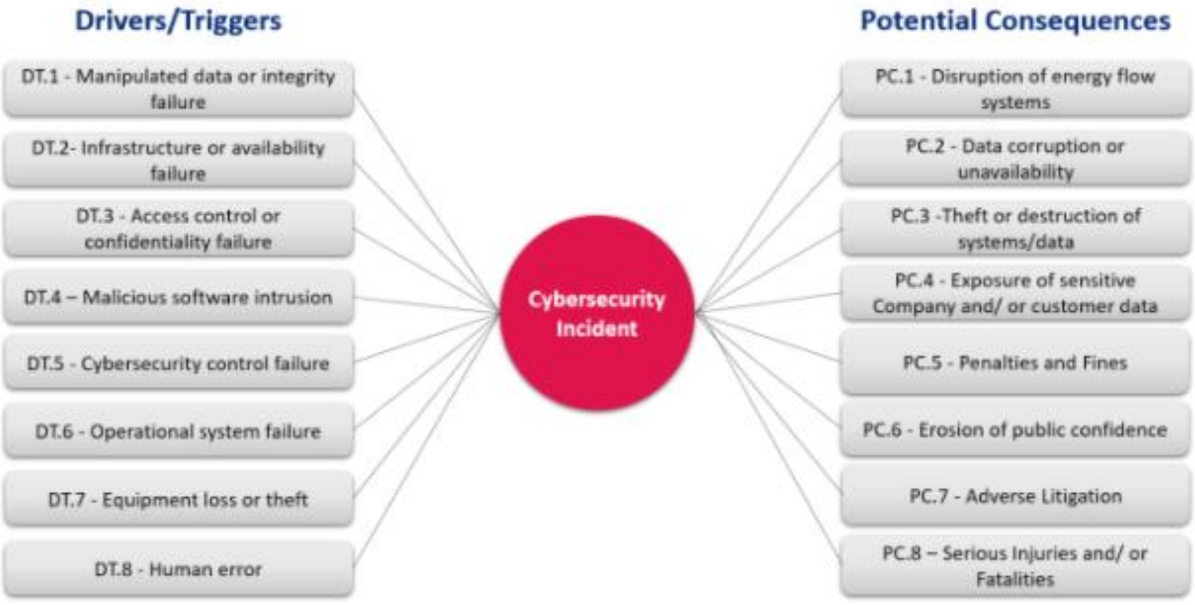
In accordance with the S-MAP Settlement Decision,[15] this section describes the risk Bow Tie, possible Drivers, potential Consequences, and the risk score for the Cybersecurity risk.

[15] D.18-12-014.

A. Risk Bow Tie and Risk Event Associated with the Risk

The risk bow tie is a commonly used tool for risk analysis, and the Settlement Decision[16] instructs the utility to include a risk bow tie illustration for each risk included in RAMP. As illustrated in the risk bow tie shown below in Figure 1, the risk event (center of the bow tie) is a cybersecurity event, the left side of the bow tie illustrates drivers/triggers that lead to a cybersecurity event, and the right side shows the potential consequences of a cybersecurity event. SoCalGas and SDG&E applied this framework to identify and summarize the information provided in Figure 1. A mapping of each mitigation to the element(s) of the risk bow tie addressed is provided in Appendix A.

Figure 1: Risk Bow Tie


Drivers/Triggers
DT.1 - Manipulated data or integrity failure
DT.2- Infrastructure or availability failure
DT.3 - Access control or confidentiality failure
DT.4 – Malicious software intrusion
DT.5 - Cybersecurity control failure
DT.6 - Operational system failure
DT.7 - Equipment loss or theft
DT.8 - Human error
Cybersecurity Incident
Potential Consequences
PC.1 - Disruption of energy flow systems
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.5 - Penalties and Fines
PC.6 - Erosion of public confidence
PC.7 - Adverse Litigation
PC.8 – Serious Injuries and/ or Fatalities

B. Overarching & Cross-Functional Factors

Cross-functional factors (CFF) refer to initiatives (drivers, consequences, and/or mitigations) that are associated with, but are not specific to, any specific RAMP risk. Cybersecurity does not operate in a vacuum. It touches upon, and its focus is, to protect every technology system in the Companies.

[16] *Id.* at Attachment A, A-11 (“Bow Tie”).

An important cross-functional factor that impacts the Cybersecurity risk is the safe and reliable operation of Foundational Technology Systems. As explained in RAMP Chapters SCG-CFF-4/SDG&E-CFF-4, these systems are used in every aspect of operations, customer engagement, and emergency response. These systems encompass the Companies' critical software application systems, communication networks, monitoring systems, end-user systems, and hardware and software platforms hosted in the Companies' data centers and on internal and external Cloud Platforms. The security and reliability of operations depend on Foundational Technology Systems; thus, it is critical for these systems to be secure, resilient, and recoverable to mitigate risks.

Cybersecurity threats, if successful, can impact the Companies' Foundational Technology Systems. Impacts to Foundational Technology Systems can negatively affect critical business operations and processes that rely on these systems. The following four factors relate to Foundational Technology Systems:

(1) Technology systems have become the foundation for operational, business, and customer engagement needs across the enterprise, where even the most routine tasks rely on an interdependent network of systems and services. The interdependencies of such systems can create an increased Cybersecurity risk.

(2) Technology can quickly become obsolete and require lifecycle management activities such as maintenance, upgrades, and replacements. Neglecting these activities may result in downstream impacts, performance issues, and/or cybersecurity vulnerabilities.

(3) The industry is faced with constantly evolving threats from both domestic and foreign adversaries, as well as supply chain risks, third-party and insider threats, and natural hazards. Collectively, the dependency on technology systems and the dynamic nature of technology threats, hazards, and risks requires that the Companies' controls and mitigations leverage the latest security solutions on the market and constantly adapt to securely, safely, and reliably provide services to the workforce and customers.

(4) Cloud technology is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—to offer faster innovation, flexible resources, and economies of scale. Implementing and operating in a secure cloud enables the use of a broad set of policies, technologies, applications, and controls provided by the Cloud

Platforms to assist in protecting sensitive Company data, applications, services, and the associated infrastructure.

Cloud technology provides a shared responsibility model between Cloud Platforms and the Company. Although the Company is ultimately accountable for ensuring cybersecurity protections are in place and effective, the Companies' Cloud Platform partners are responsible for protecting the infrastructure that runs the services offered in the cloud. Specifically, the cloud provider manages the security of the cloud, while security in the cloud is the responsibility of the Companies.

By prioritizing Cloud Platform as a service, the Companies are decreasing the Cybersecurity risk raised by traditional Information Technology (IT) systems and manual techniques. Cloud providers manage security, patching, and updates at the platform level, allowing the Companies to focus on driving business value and increasing enterprise resiliency.

C. Potential Drivers/Triggers[17]

The Settlement Decision[18] instructs the utility to identify which element(s) of the associated risk Bow Tie each mitigation addresses. When performing the risk assessment for Cybersecurity, SoCalGas and SDG&E identified potential leading indicators, referred to as Drivers or Triggers. These include, but are not limited to:

- **DT.1 - Manipulated data or integrity failure**: Any unintended changes to data as the result of a storage, retrieval or processing operation, including malicious intent, unexpected hardware failure, and human error.
- **DT.2 - Infrastructure or availability failure**: An unplanned, severe, extensive and/or large-scale system outage caused by a cybersecurity-related event or incident.
- **DT.3 - Access control or confidentiality failure**: Inability to effectively perform identification, authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.

[17] An indication that a risk could occur. It does not reflect actual or threatened conditions.

[18] D.18-12-014 at Attachment A, A-11 ("Bow Tie").

- **DT.4 - Malicious software intrusion**: Any malicious program or code that is harmful to systems. For example, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations.
- **DT.5 - Cybersecurity control failure**: A general failure of a cybersecurity control(s). *E.g.*, a vulnerability scanner ceases functioning, allowing an exploitable vulnerability to go unnoticed in the environment.
- **DT.6 - Operational system failure**: A system failure occurring due to a cybersecurity event/incident, causing the system to freeze, reboot, function counter to its design or stop functioning.
- **DT.7 - Equipment loss or theft**: A type of data breach where there is a loss of a laptop, mobile device, or storage device such as backup tapes, hard drives, and flash drives whether by accidental loss or through malicious intent.
- **DT.8 - Human error (*e.g.*, clicking on a phishing email):** An accidental cybersecurity event/incident conducted by a human.

D. Potential Consequences of Risk Event

Potential Consequences[19] are listed to the right side of the risk Bow Tie illustration provided above. If one or more of the Drivers/Triggers listed above were to result in an incident, the potential Consequences, in a reasonable worst-case scenario, could include:

- PC.1 - Disruption of energy flow systems
- 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.5 - Penalties and fines
- PC.6 - Erosion of public confidence
- PC.7 - Adverse litigation
- PC.8 – Serious injuries and/ or fatalities

[19] D.18-12-014 at 16 and Attachment A, A-8 ("Identification of Potential Consequences of Risk Event").

These potential Consequences were used in the scoring of Cybersecurity that occurred during the development of SoCalGas' and SDG&E's respective 2020 Enterprise Risk Registries.

E. Risk Score

The Settlement Decision requires a pre- and post-mitigation risk calculation.[20] Chapter RAMP-C of this RAMP Application explains the Risk Quantitative Framework that underlies this Chapter, including how the Pre-Mitigation Risk Score, Likelihood of Risk Event (LoRE), and Consequence of Risk Event (CoRE) are calculated.

Table 2: Pre-Mitigation Analysis Risk Quantification Scores[21]

SoCalGas	**LoRE**	**CoRE**	**Risk Score**
Cybersecurity	0.09	10,829	975
SDG&E	**LoRE**	**CoRE**	**Risk Score**
Cybersecurity	0.08	16,446	1,316

Pursuant to Step 2A of the Settlement Decision, the utility is instructed to use actual results, and available and appropriate data.[22] Given the emerging and evolving nature of Cybersecurity risk, particularly in the Operational Technology (OT) domain, there is limited information to assess the risk using historical information. Therefore, the Companies used multiple indicators in predicting the likelihood and consequence of such an event, such as SME and industry data to inform the likelihood and consequence values. The risk of a Cybersecurity incident was evaluated with consideration for the different risk profiles of the OT infrastructure of the gas and electric systems. Additional information and the evaluation of Cybersecurity risk and the potential gas system impacts and electric system impacts is provided in Appendix B.

III. 2020 CONTROLS

This section "[d]escribe[s] the controls or mitigations currently in place" as required by the Settlement Decision.[23] The activities in this section were in place as of December 31, 2020. Controls that will continue in 2022-2024 are addressed below in Section IV.

[20] *Id.* at Attachment A, A-11 ("Calculation of Risk").

[21] The term "pre-mitigation analysis," in the language of the S-MAP Settlement Decision (Attachment A, A-12 ("Determination of Pre-Mitigation LoRE by Tranche," "Determination of Pre-Mitigation CoRE," "Measurement of Pre-Mitigation Risk Score")), refers to required pre-activity analysis conducted prior to implementing control or mitigation activity.

[22] *Id.* at Attachment A, A-8 ("Identification of Potential Consequences of Risk Event").

[23] D.18-12-014 at 33.

The controls discussed in this chapter focus on activities performed or supported directly by the Cybersecurity department as a shared service for SoCalGas, SDG&E, and Sempra Energy. The Cybersecurity department manages cybersecurity risks across the enterprise.

The Cybersecurity program utilizes risk management frameworks, including but not limited to the National Institute of Standards and Technology (NIST) Cybersecurity 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 their planned controls. The Companies have adopted a comprehensive and enhanced control portfolio that balances risk mitigation and cost effectiveness while also establishing foundational security capabilities that will serve to mitigate risks from evolving threats. The planned controls are designed to provide adequate risk reduction to offset the projected Cybersecurity risk increase to maintain this risk at a manageable level.

A. Control 1: Perimeter Defenses

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 operational technology 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. The purpose of the defense-in-depth strategy is to manage 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 control 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.

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 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.

Accordingly, the Perimeter Defenses control addresses several Drivers/Triggers as outlined above in Figure 1 and in Appendix A including: Manipulated data or integrity failure (DT.1), Infrastructure or availability failure (DT.2), Access control or confidentiality failure (DT.3), Malicious software intrusions (DT.4), Cybersecurity control failures (DT.5), Operational system failures (DT.6), Equipment Loss or Theft (DT.7), Human error (DT.8). In addition, the Perimeter Defenses control helps to reduce the Potential Consequences of: Data corruption or unavailability (PC.2), Theft or destruction of systems/data (PC.3), Exposure of internal data (PC.4), Erosion of public confidence (PC.6).

Perimeter Defenses projects presented in this control include:

- Firewall upgrades and process automation,
- Web Application Firewall Protection,
- Distributed Denial of Service Protection,
- System security assessment efforts,
- Browser isolation/sandboxing,
- IoT (Internet of Things) Sensors, and
- Perimeter Defense mechanisms.

B. Control 2: Internal Defenses

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 assets, Foundational Technology 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 controls in this category 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 mitigations. 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 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.

Based on the foregoing, Internal Defenses address several Drivers/Triggers and Potential Consequences including: Manipulated data or integrity failure (DT.1), Infrastructure or availability failure (DT.2), Access control or confidentiality failure (DT.3), Malicious software intrusions (DT.4), Cybersecurity control failures (DT.5), Operational system failures (DT.6), Equipment Loss or Theft (DT.7), Human error (DT.8), Data corruption or unavailability (PC.2), Theft or destruction of systems/data (PC.3), Exposure of internal data (PC.4), Erosion of public confidence (PC.6).

Internal Defenses projects presented in this control include:

- Endpoint Security Monitoring,
- Threat and Vulnerability Management,
- Insider Threat Detection and User Behavior Analytics,
- Incident Management,
- Third Party External Privileged Access Management,
- Data Loss Prevention (DLP)
- Supply Chain Risk Management, and
- Cloud Access Security

C. Control 3: Sensitive Data Protection

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 control 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 control will help the Companies continue the prudent management of sensitive data.

Sensitive Data Protection addresses several Drivers/Triggers and Potential Consequences including: Manipulated data or integrity failure (DT.1), Access control or confidentiality failure (DT.3), Cybersecurity control failures (DT.5), Human error (DT.8), Data corruption or unavailability (PC.2), Theft or destruction of systems/data (PC.3), Exposure of internal data (PC.4), Penalties and fines (PC.5), Erosion of public confidence (PC.6), Adverse litigation (PC.7).

The Companies' current control activities target sensitive data within information technology systems, including laptops and other mobile computing devices. Sensitive Data Protection controls are designed to include:

- Identity Access Management Enhancements,
- Data Loss Prevention & Enhancements,
- Forensics Infrastructure Enhancements,
- Mobile Device Security, and
- Data Crawler Technology.

D. Control 4: Operational Technology (OT) Cybersecurity

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. Network anomaly detection, endpoint detection, and security event monitoring improves visibility into the OT environment, which allows for faster response and remediation. Enhanced secure access technologies help reduce risk of unauthorized access. These risk mitigation activities strengthen our 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.

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. Anomaly detection, endpoint detection, and security event monitoring improves visibility into the OT environment, which allows for faster response and remediation. Enhanced secure access technologies help reduce risk of unauthorized access. These risk mitigation 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.

This specialized OT Cybersecurity addresses several Drivers/Triggers and Potential Consequences including: Infrastructure or availability failure (DT.2), Access control or confidentiality failure (DT.3), Malicious software intrusions (DT.4), Cybersecurity control failures (DT.5), Operational system failures (DT.6), Human error (DT.8), Disruption of energy flow systems (PC.1), Data corruption or unavailability (PC.2), Penalties and fines (PC.5), Erosion of public confidence (PC.6), Adverse litigation (PC.7), Serious Injuries and Fatalities (PC.8).

The Companies' cybersecurity program prioritizes operational technology controls, 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 Companies' OT Cybersecurity projects presented in this control include:

- OT Cybersecurity Tools Hosting Environment Enhancements
- OT Network Anomaly Detection
- OT Application Whitelisting
- OT Advanced Security Incident Management (SIEM) and Analytics
- OT Asset Inventory Control
- OT Environment Network Access Control
- OT Environment Endpoint Detection Response
- OT Network Anomaly Detection Critical Facilities
- OT Malware Defense
- OT Secure Remote Connection

E. Control 5: Obsolete Information Technology (IT) Infrastructure and Application Replacement

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 obsolete technologies that lead to security risks. This is frequently referred to as "Foundational Technology Systems Lifecycle Management."

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.

In addition, there are fundamental control activities required to support and effectively manage the cybersecurity capabilities listed in the previous sections. These baseline activities referenced in the O&M (Operations & Maintenance) budget outlook (see Tables 4 and 5 below) support the capital investments. Some examples of these baseline controls include, but are not limited to:

- A security policy framework
- Risk management and assessments
- Cybersecurity awareness and training
- Security assessment
- Asset 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

Obsolete IT Infrastructure and Application Replacement addresses several Drivers/Triggers and Potential Consequences as outlined above in Figure 1 and in Appendix A. These include: Manipulated data or integrity failure (DT.1), Infrastructure or availability failure (DT.2), Access control or confidentiality failure (DT.3), Malicious software intrusions (DT.4), Cybersecurity control failures (DT.5), Operational system failures (DT.6), Disruption of energy flow systems (PC.1), Data corruption or unavailability (PC.2), Theft or destruction of systems/data (PC.3), Exposure of sensitive Company and customer data (PC.4), Erosion of public confidence (PC.6).

The projects presented in this control include:

- Technology refreshes, including, but not limited to:
   - Infrastructure
   - Operating systems
   - Middleware
   - Applications
- System maintenance to confirm continued secure configurations, patching, upgrading, among others.
- Use of effective architecture and other mechanisms to confirm high availability and service continuity for critical systems.

IV. 2022-2024 CONTROL & MITIGATION PLAN

This section contains a table identifying the controls and mitigations comprising the portfolio of mitigations for this risk.[24] All of the activities discussed in Section III above are expected to continue during the TY 2024 GRC. For clarity, a current activity that is included in the 2022-2024 plan may be referred to as either a control and/or a mitigation. For purposes of this RAMP, a control that will continue as a mitigation will retain its control ID unless the size and/or scope of that activity will be modified, in which case that activity's control ID will be replaced with a mitigation ID. The table below shows which activities are expected to continue.

[24] *See id.* at Attachment A, A-14 ("Mitigation Strategy Presentation in the RAMP and GRC").

Table 3 Mitigation Plan Summary

Line No.	Control/ Mitigation ID	Control/Mitigation Description	2020 Controls	2022-2024 Plan
1	C1	Perimeter Defenses	X	X
2	C2	Internal Defenses	X	X
3	C3	Sensitive Data Protection	X	X
4	C4	OT Cybersecurity	X	X
5	C5	Obsolete IT Infrastructure and Asset Replacement	X	X

A single tranche is appropriate for a Cybersecurity risk event, as there is no logical disaggregation of assets or systems related to the controls presented in the mitigation plan. The controls for this risk are evaluated at the program level due to the availability of data, the rapidly changing threats, and applicable counter measures. As mentioned in the Risk Overview section above, sharing specific details of the individual risk mitigation activity can provide adversaries crucial information that could aid their ability to disrupt Company systems. Therefore, the level of granularity for quantifying RSE (Risk Spend Efficiency) is currently at the operational program level (*i.e.*, Perimeter Defenses, Internal Defenses, Sensitive Data Protection, OT Cybersecurity and Obsolete IT Infrastructure and Asset Replacement) rather than each individual risk mitigation activity for the Cybersecurity risk.

A. Changes to 2020 Controls

The Companies plan to continue each of the existing controls discussed above in Section III through the 2022 – 2024 period without any significant changes.

B. 2022 – 2024 Mitigations

The Companies are currently not planning any new mitigations during the 2022 – 2024 period.

V. COSTS, UNITS, AND QUANTITATIVE SUMMARY TABLES

The tables in this section provide a summary of the risk mitigation plan, including the associated costs, units, and the RSEs, by tranche. SoCalGas and SDG&E do not account for and track costs by activity or tranche; rather, SoCalGas and SDG&E account for and tracks costs by cost center and capital budget code. The costs shown were estimated using assumptions provided by SMEs and available accounting data.

Table 4: SoCalGas Risk Control and Mitigation Plan - Recorded and Forecast Dollars Summary[25]
(Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Recorded Dollars		Forecast Dollars			
		2020 Capital	2020 O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 O&M (Low)	TY 2024 O&M (High)
C1	Perimeter Defenses	$8,037	$1,032	$10,445	$13,347	$1,251	$1,599
C2	Internal Defenses	$4,658	$3,124	$10,816	$13,821	$3,158	$4,035
C3	Sensitive Data Protection	$0	$2,377	$7,054	$9,014	$2,351	$3,004
C4	OT Cybersecurity	$127	$896	$14,790	$18,898	$1,066	$1,362
C5	Obsolete IT Infrastructure and Asset Replacement	$206	$1,083	$8,928	$11,408	$1,297	$1,657

[25] Recorded costs and forecast ranges are rounded. Additional cost-related information is provided in workpapers. Costs presented in the workpapers may differ from this table due to rounding. The figures provided are direct charges and do not include company loaders, with the exception of vacation and sick. The costs are also in 2020 dollars and have not been escalated to 2021 amounts. The capital presented is the sum of the years 2022, 2023, and 2024, or a three-year total. Years 2022, 2023 and 2024 are the forecast years for the Company's Test Year 2024 GRC Application.

Table 5: SDG&E Risk Control and Mitigation Plan - Recorded and Forecast Dollars Summary[26]
(Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Recorded Dollars		Forecast Dollars			
		2020 Capital	2020 O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 O&M (Low)	TY 2024 O&M (High)
C1	Perimeter Defenses	$10,231	$811	$10,013	$12,795	$984	$1,257
C2	Internal Defenses	$4,312	$2,457	$9,405	$12,018	$2,483	$3,173
C3	Sensitive Data Protection	$0	$1,869	$6,807	$8,698	$1,849	$2,362
C4	OT Cybersecurity	$458	$704	$16,245	$20,758	$838	1,071
C5	Obsolete IT Infrastructure and Asset Replacement	$1,326	$852	$7,921	$10,121	$1,020	$1,303

[26] *See*, *supra*, n. 25.

Table 6: SoCalGas Risk Control & Mitigation Plan - Units Summary

ID	Control/Mitigation Name	Units Description		Recorded Units		Forecast Units			
		Capital	O&M	2020 Capital	2020 O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 (Low) O&M	TY 2024 (High) O&M
C1	Perimeter Defenses	The cybersecurity mitigations have multiple different types of units of measure. For example, in the Perimeter Security mitigation area there are devices involved, network users, data consumed, service contracts, etc. It would not be accurate or consistent to identify a single unit of measure.							
C2	Internal Defenses								
C3	Sensitive Data Protection								
C4	OT Cybersecurity								
C5	Obsolete IT Infrastructure and Asset Replacement								

Table 7: SDG&E Risk Control & Mitigation Plan - Units Summary

ID	Control/Mitigation Name	Units Description		Recorded Units		Forecast Units			
		Capital	O&M	2020 Capital	2020 O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 (Low) O&M	TY 2024 (High) O&M
C1	Perimeter Defenses	The cybersecurity mitigations have multiple different types of units of measure. For example, in the Perimeter Security mitigation area there are devices involved, network users, data consumed, service contracts, etc. It would not be accurate or consistent to identify a single unit of measure.							
C2	Internal Defenses								
C3	Sensitive Data Protection								
C4	OT Cybersecurity								
C5	Obsolete IT Infrastructure and Asset Replacement								

Table 8: SoCalGas Risk Control & Mitigation Plan - Quantitative Analysis Summary (Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast			
		LoRE	CoRE	Risk Score	RSE
C1	Perimeter Defenses	0.10	13,482	1,356	160
C2	Internal Defenses	0.11	13,482	1,544	95
C3	Sensitive Data Protection	0.14	13,482	1,918	62
C4	OT Cybersecurity	0.05	10,829	497	112
C5	Obsolete IT Infrastructure and Asset Replacement	0.13	13,482	1,731	102

Table 9: SDG&E Risk Control & Mitigation Plan - Quantitative Analysis Summary
(Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast			
		LoRE	CoRE	Risk Score	RSE
C1	Perimeter Defenses	0.10	13,482	1,356	160
C2	Internal Defenses	0.11	13,482	1,544	95
C3	Sensitive Data Protection	0.14	13,482	1,918	62
C4	OT Cybersecurity	0.04	16,466	672	142
C5	Obsolete IT Infrastructure and Asset Replacement	0.13	13,482	1,731	102

VI. ALTERNATIVES

Pursuant to D.14-12-025 and D.16-08-018, the Companies considered alternatives to the risk mitigation plan for the Cybersecurity risk. The risk mitigation plan for the Cybersecurity risk is defined as the planned portfolio of control programs. Typically, analysis of alternatives occurs when designing the portfolio to obtain the best result or product for the cost. The alternatives analysis considered modifications to the risk mitigation plan and constraints, such as budget and resources.

The Companies considered two alternative portfolios of mitigation activities in addition to the planned portfolio control program to address the Companies' Cybersecurity risk. The alternative portfolios were analyzed in the context of risk-spend efficiency, as outlined in the tables below.

For the alternative analysis, the Companies analyzed the effectiveness of three portfolios:

1. The risk mitigation plan for the Cybersecurity risk,
2. Alternative Portfolio 1, and
3. Alternative Portfolio 2.

To create these three different portfolios, the Companies first assessed the potential impact of each capital project under consideration, identifying each as high/medium/low based on several criteria:

- The project implementation's impact on the maturity of cybersecurity at the Companies;

- The extent to which each project addresses recommendations from CSC 20,[27] ICS-CERT,[28] and other frameworks;
- The extent to which each project addresses threats to cybersecurity of high impact and likelihood; and
- The effectiveness in mitigating a credible attack impacting safety.

After each project was tagged as High/Medium/Low, the following three portfolios were developed: The risk mitigation plan for the Cybersecurity risk, Alternative Portfolio 1 and Alternative Portfolio 2.

A. The Risk Mitigation Plan for the Cybersecurity risk

The Companies' risk mitigation plan includes a mix of "high" impact and "medium" impact projects. The identified high-impact and medium-impact projects were grouped into the five programs described above:

1. Perimeter Defenses,
2. Internal Defenses,
3. Sensitive Data Protection,
4. Operational Technology Cybersecurity, and
5. Obsolete IT Infrastructure and Application Replacement.

The quantitative analysis conducted by the Companies shows that the Companies' Plan of high- and medium-impact projects is the most cost-effective portfolio for managing the increase in Cybersecurity risk, as is demonstrated by the high RSE compared to other alternative portfolios.

[27] CSC-20: The Twenty (20) Critical Security Controls (CSC) for Cyber Defense are a culmination of exhaustive research and development of information security initiatives that advocate a "offense must inform defense approach," as noted by the SANS institute, available at *https://www.sans.org/critical-security-controls*.

[28] ICS-CERT: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT (*https://us-cert.cisa.gov/ics*) to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

B. Alternative Portfolio 1

The Companies' Alternative Portfolio 1 consists of "high" impact projects only. The identified high-impact projects were grouped into the same five programs described above. The quantitative analysis conducted by the Companies shows that the Companies' Alternative Portfolio 1, comprising only high-impact projects, is estimated to have a lower RSE than the Plan when considering the RSE of the individual categories, as shown below. In addition, this portfolio does not provide enough risk reduction to address the increasing rate of Cybersecurity risk. The effectiveness of the projects in this alternative portfolio is lower than the growth rate of the risk. If Alternative Portfolio 1 is executed, the Cybersecurity risk will increase compared to the Companies' risk mitigation plan.

The quantitative analyses for each of the five utility-focused operational cybersecurity categories are presented below. As stated above, these projects, when combined into an alternative portfolio, is lower than the Companies' Plan.

1. Alternative Portfolio 1 – C1 (High-impact Perimeter Defenses)
2. Alternative Portfolio 1 – C2 (High-impact Internal Defenses)
3. Alternative Portfolio 1 – C3 (High-impact Sensitive Data Protection)
4. Alternative Portfolio 1 – C4 (High-impact OT Cybersecurity)
5. Alternative Portfolio 1 – C5 (High-impact Obsolete IT Infrastructure and Application Replacement)

C. Alternative Portfolio 2

Alternative Portfolio 2 consists of all cybersecurity projects under consideration (*i.e.,* high-impact, medium-impact and low-impact). Whereas the Companies' risk mitigation plan includes high- and medium-impact projects, and Alternative Portfolio 1 includes only high-impact projects, Alternative Portfolio 2 includes all projects that the Companies have currently identified. Alternative Portfolio 2 has the highest cost, with the most risk reduction. Alternative Portfolio 2 has an RSE lower than the Companies' Plan since the additional projects in the portfolio (the low-impact projects not included in the Companies' risk mitigation plan for the Cybersecurity risk) provide an incremental benefit; however, that incremental benefit is less effective relative to its incremental cost.

1. Alternative Portfolio 2 – C1 (High-, Medium-, and Low-impact Perimeter Defenses)

2. Alternative Portfolio 2 – C2 (High-, Medium-, and Low-impact Internal Defenses)

3. Alternative Portfolio 2 – C3 (High-, Medium-, and Low-impact Sensitive Data Protection)

4. Alternative Portfolio 2 – C4 (High-, Medium-, and Low-impact OT Cybersecurity)

5. Alternative Portfolio 2 – C5 (High-, Medium-, and Low-impact Obsolete IT Infrastructure and Application Replacement)

The costs and RSEs for Alternative Portfolio 1 and Alternative Portfolio 2 are presented in the tables that follow.

Table 10: SoCalGas Alternate Mitigation Plan - Recorded and Forecast Dollars Summary[29] (Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast Dollars			
		2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 O&M (Low)	TY 2024 O&M (High)
A1	Alternative Portfolio 1	$47,984	$61,312	$9,122	$11,656
A2	Alternative Portfolio 2	$81,319	$103,907	$9,122	$11,656

Table 11: SDG&E Alternate Mitigation Plan - Recorded and Forecast Dollars Summary[30] (Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast Dollars			
		2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 O&M (Low)	TY 2024 O&M (High)
A1	Alternative Portfolio 1	$20,159	$25,759	$7,173	$9,166
A2	Alternative Portfolio 2	$21,104	$26,966	$7.173	$9,166

[29] *See, supra*, n. 25.

[30] *Id.*

Table 12: SoCalGas Alternate Mitigation Plan - Units Summary

ID	Alternative Mitigation Name	Units Description		Forecast Units			
		Capital	O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 (Low) O&M	TY 2024 (High) O&M
A1	Alternative Portfolio 1	The cybersecurity mitigations have multiple different types of units of measure. For example, in the Perimeter Security mitigation area there are devices involved, network users, data consumed, service contracts, etc. It would not be accurate or consistent to identify a single unit of measure.					
A2	Alternative Portfolio 2						

Table 13: SDG&E Alternate Mitigation Plan - Units Summary

ID	Alternative Mitigation Name	Units Description		Forecast Units			
		Capital	O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 (Low) O&M	TY 2024 (High) O&M
A1	Alternative Portfolio 1	The cybersecurity mitigations have multiple different types of units of measure. For example, in the Perimeter Security mitigation area there are devices involved, network users, data consumed, service contracts, etc. It would not be accurate or consistent to identify a single unit of measure.					
A2	Alternative Portfolio 2						

Table 14: SoCalGas Alternate Mitigation Plan - Quantitative Analysis Summary (Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast			
		LoRE	CoRE	Risk Score	RSE
A1-C1	Perimeter Defenses	0.12	13,482	1610	157
A1-C2	Internal Defenses	0.13	13,482	1746	85
A1-C3	Sensitive Data Protection	0.15	13,482	2019	56
A1-C4	OT Cybersecurity	0.06	10,829	627	110
A1-C5	Obsolete IT Infrastructure and Application Replacement	0.14	13,482	1883	98
A2-C1	Perimeter Defenses	0.09	13,482	1238	154
A2-C2	Internal Defenses	0.11	13,482	1449	88
A2-C3	Sensitive Data Protection	0.14	13,482	1899	57
A2-C4	OT Cybersecurity	0.04	10,829	474	112
A2-C5	Obsolete IT Infrastructure and Application Replacement	0.13	13,482	1703	98

Table 15: SDG&E Alternate Mitigation Plan - Quantitative Analysis Summary (Direct After Allocations, In 2020 $000)

ID	Control/Mitigation Name	Forecast			
		LoRE	CoRE	Risk Score	RSE
A1-C1	Perimeter Defenses	0.12	13,482	1610	157
A1-C2	Internal Defenses	0.13	13,482	1746	85
A1-C3	Sensitive Data Protection	0.15	13,482	2019	56
A1-C4	OT Cybersecurity	0.05	16,465	847	110
A1-C5	Obsolete IT Infrastructure and Application Replacement	0.14	13,482	1883	98
A2-C1	Perimeter Defenses	0.09	13,482	1238	154
A2-C2	Internal Defenses	0.11	13,482	1449	88
A2-C3	Sensitive Data Protection	0.14	13,482	1889	57
A2-C4	OT Cybersecurity	0.04	16,466	672	139
A2-C5	Obsolete IT Infrastructure and Application Replacement	0.13	13,482	1703	98

APPENDIX A: SUMMARY OF ELEMENTS OF THE RISK BOW TIE

Appendix A: Summary of Elements of the Risk Bow Tie
Cybersecurity: Summary of Elements of the Risk Bow Tie

Control ID	Control Name	Elements of the Risk Bow Tie Addressed
C1	Perimeter Defenses	DT.1, DT.2, DT.3, DT.4, DT.5, DT.6, DT.7, DT.8 PC.2, PC.3, PC.4, PC.6
C2	Internal Defenses	DT.1, DT.2, DT.3, DT.4, DT.5, DT.6, DT.7, DT.8 PC.2, PC.3, PC.4, PC.6
C3	Sensitive Data Protection	DT.1, DT.3, DT.5, DT.8, PC.2, PC.3, PC.4, PC.5, PC.6, PC.7
C4	Operational Technology (OT) Cybersecurity	DT.2, DT.3, DT.4, DT.5, DT.6, DT.8 PC.1, PC.2, PC.5, PC.6, PC.7, PC.8
C5	Obsolete Information Technology (IT) Infrastructure and Application Replacement	DT.1, DT.2, DT.3, DT.4, DT.5, DT.6, PC.1, PC.2, PC.3, PC.4, PC.6

APPENDIX B: QUANTITATIVE ANALYSIS SOURCE DATA REFERENCES

Appendix B: Quantitative Analysis Source Data References

Cybersecurity: Quantitative Analysis Source Data References

The Settlement Decision directs the utility to identify potential consequences of a risk event using available and appropriate data.[31] The list below provides the inputs used as part of this assessment.

Gas Systems Impacts

The scoring for a cybersecurity attack's impact on the gas system was conducted using SME input and industry data as a proxy for historical cybersecurity attacks on the gas system. A number of potential cybersecurity attacks on the gas system were evaluated to determine safety, financial, and reliability consequences of an event. A cybersecurity attack with high safety consequences could involve the inundation of the Companies' Contact Centers (call center) by attackers, rendering the call centers inoperable. This might prevent customers and employees from being able to alert the Companies about time-sensitive gas operations emergencies in the field. Which, in turn, could result in a delayed Company response to the gas emergency, exacerbating the safety and reliability consequences of the event. For example, a gas leak, if left unreported and unremedied, under some circumstances might lead to an explosion or ignition. To determine the safety impacts of a cybersecurity attack on a call center, the Companies relied on historical Company evacuations data to estimate the number of customers who may not be evacuated during a gas leak if unable to contact the Company due to a cybersecurity attack on the call center. The financial consequences of a cybersecurity attack on the call center include the cost of stolen customer records, as informed by Ponemon Institute's 2020 "Cost of a Data Breach Report."[32] In addition to financial consequences, the theft of customer records can lead to reputational consequences for the Company.

A cybersecurity attack on the gas system may result in the attacker gaining access to the gas control or Supervisory Control And Data Acquisition (SCADA) systems and manipulating, or disarming alarms to cause operational and safety consequences. The 2008 Turkey Oil Pipeline explosion is a historical example of this type of cybersecurity attack. During this attack,

[31] D.18-12-014, Attachment A at A-8 (Identification of Potential Consequences of Risk Event).

[32] *See*, DigitalGuardian, *What Does a Data Breach Cost in 2020?* (August 18, 2020), available at *https://digitalguardian.com/blog/what-does-data-breach-cost-2020.*

attackers gained access to the pipeline's surveillance systems and valve stations and over-pressured the pipeline without triggering alarms.[33] The overpressure resulted in an explosion that cost over a million dollars and resulted in thousands of barrels of oil spilled near a water aquifer. To determine the safety impacts of a cybersecurity attack impacting gas control at the Companies, SMEs analyzed the safety consequences of national Pipeline and Hazardous Materials Safety Administration (PHMSA) transmission incident events without SCADA in place. The average value of safety impacts for these events was used as a proxy for a cybersecurity attack on the gas control system at the Companies. Financial consequences for an attack on the gas control/SCADA systems were informed by industry research, including a Center for Strategic and International Studies report, which calculated the cost of a cybersecurity attack on oil and gas SCADA systems at an estimated $8.4 million per day.[34] SME input estimates the time to rebuild the SCADA system as one month in a worst-case scenario. A cybersecurity attack on the gas control center can also have major reliability consequences. To determine the operational consequences of this type of event, SMEs used the average reliability impacts of incidents on the transmission system at the Companies (*see* Incident Related to the High Pressure System (Excluding Dig-in) RAMP chapters SCG-Risk-1/SDG&E-Risk-3). A cybersecurity attack may result in outages and lead to a gas curtailment.

Several data points and sources were used by the Companies' SMEs to estimate the likelihood of events on the electric and gas systems. According to the 2015 Lloyd's Emerging Risk Report, "there have been 15 suspected cyber attacks or events on the US electricity grid since 2000"[35] to 2015. The estimate of the likelihood of this event occurring based on that report is in the order of 2% (1 in 50 years). In addition, a 2017 industry research report by Accenture,

[33] Bloomberg, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar* (December 10, 2014), available at *https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.*

[34] McAfee, Inc. *In The Crossfire: Critical Infrastructure In The Age of Cyber War* (2010), available at *https://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf.*

[35] Lloyd's Emerging Risk Report – 2015, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid* (2015) at 53, available at *https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.*

"Cost of Cyber Crime Study,"[36] indicates a rapidly evolving risk increasing at an annual rate of 27%. The 2019 study reflected a similar rate of increase at 11%. Given this information, the Companies' SMEs provide a likelihood of 2% for the cyber risk or 1:50 years. This frequency was also used as a proxy for cybersecurity attacks on the gas system with low safety consequences, such as attacks on the gas control center. An attack with high safety consequences on the gas system, such as an attack on a Company Contact Center, was given a frequency of 1 incident in 25 years based on SME input.

Electric System Impacts

To determine the potential consequences for the electric system, SMEs evaluated relevant industry event scenarios to determine a credible worst-case scenario of a cybersecurity attack at SDG&E. Historical examples used to inform estimates of potential consequences of a cybersecurity attack on the electric system include:

- Ukraine (2015 and 2016) – In 2015, remote cyber intrusions caused outages at three regional electric power distribution companies, impacting approximately 225,000 customers for 6 hours in Ukraine. In 2016, hackers used a more sophisticated malware ("Crash Override") in an attempt to disable protective relay devices through a denial of service (DoS) attack. Although the 2016 attack only caused a one-hour outage, recent research suggests that hackers intended to inflict lasting damage that could have led to outages for weeks or even months.
- Southwest US Outage (2011) – In 2011, a maintenance procedure in Yuma, Arizona caused a cascade of power failures across the Southwest resulting in widespread outages in SDG&E's service territory. As the failure spread, grid operators were unaware of many rapid-fire events outside their territories. Electrical service was restored to most of SDG&E's customers within 12 hours.
- Northeast US Outage (2003) – The biggest blackout in North America occurred in 2003. High voltage power lines came into contact with vegetation, and a

[36] Ponemon Institute, LLC and Accenture, *2017 Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference* (2017) at 2, ("*... 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.*

combination of human error and equipment failures resulted in outages for 50 million people.

- Lloyds Scenarios (Scenario 1) – A report produced by Lloyd’s of London and the University of Cambridge considered the impact of a hypothetical cybersecurity attack. In the scenario, malware infects generation control rooms in the Northeast US. The malware goes undetected until triggered and tries to take control of generators. While power is restored to some areas within 24 hours, others remain without electricity for weeks.