Risk Assessment Mitigation Phase
(Chapter SDG&E-10/SCG-9)
Cybersecurity

November 27, 2019

TABLE OF CONTENTS

Risk: Cybersecurity

I. INTRODUCTION

The purpose of this chapter is to present the risk mitigation plan San Diego Gas & Electric Company (SDG&E) and Southern California Gas Company (SoCalGas) (collectively, the Companies) for the risk of Cybersecurity. This risk chapter is identical for both Companies given that the Cyber risk is currently managed centrally at the 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 (the SA Decision).[1]

The Companies 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, the Companies' Enterprise Risk Management (ERM) organization facilitates the Enterprise Risk Registry (ERR) process, which influenced how risks were selected for inclusion in this 2019 RAMP Report, consistent with the SA Decision's directives.

The purpose of RAMP is not to request funding. Any funding requests will be made in SDG&E's and SoCalGas' respective General Rate Case (GRC) applications. The costs presented in this 2019 RAMP Report are those costs for which the Companies' anticipate requesting recovery in their respective Test Year (TY) 2022 GRCs. The Companies' TY 2022 GRC presentations will integrate developed and updated funding requests from the 2019 RAMP Report, supported by witness testimony.[2] For this 2019 RAMP Report, the baseline costs are the costs incurred in 2018, as further discussed in Chapter RAMP-A. This 2019 RAMP Report

---

[1] D.16-08-018 also adopted the requirements previously set forth in D.14-12-025. D.18-12-014 adopted the Safety Model Assessment Proceeding (S-MAP) Settlement Agreement with modifications and contains the minimum required elements to be used by the utilities for risk and mitigation analysis in the RAMP and GRC.

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

presents capital costs as a sum of the years 2020, 2021 and 2022 as a three-year total; whereas, O&M costs are only presented for TY 2022.

Costs for each activity that directly addresses each risk are provided where those costs are available and within the scope of the analysis required in this RAMP Report. Throughout this 2019 RAMP Report activities are delineated between controls and mitigations, consistent with the definitions adopted in the SA 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 the Companies' Cybersecurity risk; however, many of the activities presented herein also help mitigate other risk areas as outlined in Chapter RAMP-A.

As discussed in Chapter RAMP-D, Risk Spend Efficiency (RSE) Methodology, no RSE calculation is provided where costs are not available or not presented in this RAMP Report (including costs for activities that are outside of the GRC and certain internal labor costs). Additionally, the Companies did not perform RSE calculations on mandated activities. Mandated activities are defined as activities conducted to meet a mandate or law, such as a Code of Federal Regulation (CFR), Public Utilities Code, or General Order. Activities with no RSE score presented in this 2019 RAMP Report are identified in Section VII below.

The Companies have also included a qualitative narrative discussion of certain risk mitigation activities that would otherwise fall outside of the RAMP Report's requirements, to aid the California Public Utilities Commission (CPUC or Commission) and stakeholders in developing a more complete understanding of the breadth and quality of the Companies' mitigation activities. These distinctions are discussed in the applicable control/mitigation narratives in Section V. Similarly, a narrative discussion of certain "mitigation" activities and their associated costs is provided for certain activities and programs that may indirectly address

[3] *Id*. at 16.

[4] *Id.* at 17.

the risk at issue, even though the scope of the risk as defined in the RAMP Report may technically exclude the mitigation activity from the RAMP analysis. This additional qualitative information is provided in the interest of full transparency and understandability, consistent with guidance from Commission staff and stakeholder discussions.

A. Risk Definition

For purposes of this 2019 RAMP Report, 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) and/or damage or disruption to the Companies' operations (*e.g.,* Human Resources, payroll, billing), reputation, or disclosure of sensitive customer or Company data.

B. Summary of Elements of the Risk Bow Tie

Pursuant to the SA Decision,[5] for each Control and Mitigation presented herein, the Companies have identified which element(s) of the Bow Tie the risk mitigation activity addresses. Below is a summary of these elements.

Table 1: Summary of Risk Bow Tie Elements

ID	Description of Drivers/Triggers and Potential Consequences
DT.1	Manipulated data or integrity failure
DT.2	Infrastructure or availability failure
DT.3	Access control or confidentiality failure
DT.4	Malicious software intrusions
DT.5	Cybersecurity control failures
DT.6	Operational system failures
DT.7	Equipment loss or theft
DT.8	Human error
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 customer data
PC.5	Adverse litigation
PC.6	Regulatory non-compliance fines and/or sanctions
PC.7	Erosion of public confidence
PC.8	Human Injury

[5] *Id.* at Attachment A, A-11 ("Bow Tie").

C. Summary of Risk Mitigation Plan

The Companies' Risk Mitigation Plan for the Cybersecurity risk consists of five utility-focused operational cybersecurity categories:

1. Perimeter Defenses;
2. Internal Defenses;
3. Sensitive Data Protection;
4. Operational Technology (OT) Cybersecurity; and
5. Obsolete Information Technology (IT) Infrastructure and Application Replacement.

The Companies' Risk Mitigation Plan includes both baseline controls and new mitigation activities. Based on the foregoing assessment, the Companies' set forth future mitigations. In the previous RAMP filing, the Cybersecurity mitigation plan was structured using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to group like security controls. In this 2019 RAMP Report, the Companies are using operational groups to describe, and group mitigations in a more business-aligned approach. More detail can be found in Section V, below. A summary of the operational categories includes:

1. Perimeter Defenses

Enhancements to the Companies' existing Perimeter Defenses, privileged access management, firewall solutions for web applications and penetration testing consulting services to improve our solutions' ability to defend against an advanced, intelligent adversary.

2. Internal Defenses

Enhancements designed to detect and prevent malicious users (and/ or code from propagating) inside of the perimeter.

3. Sensitive Data Protection

Enhancements of security controls that will protect sensitive data throughout the technology systems.

4. **Operational Technologies (OT) Cybersecurity**

   Enhancements to the management and protection of operational technology assets, improving threat intelligence and vulnerability management, and securing the communication infrastructure.

5. **Obsolete Information Technology (IT) Infrastructure and Application Replacement**

   Enhancements to Information Technology (IT) components and capabilities that present cybersecurity risks to the Companies addressed via the necessary replacement and/or upgrades of obsolete and vulnerable IT operating systems, software, applications, hardware, monitoring tools, and other infrastructure components.

Pursuant to the SA Decision,[6] the Companies have performed a detailed pre- and post-mitigation analysis of controls and mitigations for each risk selected for inclusion in RAMP, as further described below. The Companies' 2018 Controls for this risk consist of the following:

Table 2: Summary of Controls

ID	Control Name
SDG&E-10-C1 SCG-9-C1	Perimeter Defenses
SDG&E-10-C2 SCG-9-C2	Internal Defenses
SDG&E-10-C3 SCG-9-C3	Sensitive Data Protection
SDG&E-10-C4 SCG-9-C4	Operational Technology (OT) Cybersecurity
SDG&E-10-C5 SCG-9-C5	Obsolete Information Technology (IT) Infrastructure and Application Replacement

[6] *Id.* at Attachment A, A-11 ("Definition of Risk Events and Tranches").

Finally, pursuant to the SA Decision,[7] the Companies considered alternatives to the Risk Mitigation Plan for the Cybersecurity risk and we summarize the reasons that the alternatives were not included in the Risk Mitigation Plan discussed in Section VIII, below.

D. Sensitive, Confidential Information to Be Protected

What is unique about the Cybersecurity risk, as compared to other risks driven by operations, asset management, or natural hazards, is that there is an intelligent adversary that is attempting to 1) understand the Companies' controls and 2) gain access to Company systems or information to achieve the adversary's objectives. It is important for our stakeholders to understand that some information about the Companies' mitigation plans or our worst-case scenarios would be useful to an adversary – and would indirectly harm our stakeholders. While some of our controls and strategies are considered standard practice, publishing some of these controls, intelligence, strategies, or tactics in the public record could aid our enemy, the criminal gang or nation state that is attempting to disrupt our systems and society. Sensitive details noted herein are available upon Commission request for discussion in person.

II. RISK OVERVIEW

Cybersecurity threats continue to rapidly evolve. As such, our strategy to counter cybersecurity threats must be flexible and allow us to adapt to these evolving threats over time.

Timely and accurate cybersecurity threat intelligence is key to staying abreast of this rapidly evolving threat landscape. We obtain cybersecurity threat intelligence from a variety of entities and sources, including Information Sharing and Analysis Centers (ISACs), the Federal Bureau of Investigations (FBI), the Federal Energy Regulatory Commission (FERC), the Department of Energy (DOE), the Department of Homeland Security (DHS) and a variety of United States (US) Intelligence Community agencies. Information from threat intelligence in the utility industry continues to reveal adversaries that are using advancing tradecraft to try and access our nation's utility systems.

[7] *Id.* at 33.

A. The Companies are Faced with an Evolving Cybersecurity Threat

At the FERC 2018 Reliability Technical Conference;[8] "Addressing the Evolving Cybersecurity Threat" panel, it was noted that, "There is a widespread understanding among policymakers and industry that cyberattacks are a persistent and growing threat to the reliable or resilient operation of the Bulk-Power System."[9]

A representative sample of recent threats facing our industry are provided below:

OT Attacks on Utility Infrastructure

- ***Attack on Ukrainian Electric Operator*** (https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01) 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.
- ***May 2019 reporting on Western Energy Firm attack*** (https://www.dispersive.io/blog/first-of-its-kind-denial-of-service-attack-on-western-u.s.-utility) A distributed denial of service (DDOS) attack aimed at a Northwestern US power company, disrupted operations but did not result in a loss of electric load.

Insider Attacks

- ***Capital One former insider*** (https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says) 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.

---

[8] Federal Energy Regulatory Commission, Supplemental Notice of Technical Conference (July 17, 2018), *available at* https://www.ferc.gov/CalendarFiles/20180724131230-notice-AD18-11.pdf.

[9] *Id.* at 5.

Supply Chain

- ***Russian attack on electric utility suppliers*** *(*https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112*)*

  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

- ***NotPetya*** *(*https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*)* A Russian-driven attack on IT systems, using "ransomware" malicious software that resulted in damages to the IT hardware after infection.

B. Adversaries

The adversaries the Companies face include various 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 more sophisticated set of tools and strategies to conduct attacks on the energy sector. Their suite of capabilities was touched on above but also includes advanced malware, more complex phishing attacks, among others. Adversaries are also conducting other campaigns to target utility employees, akin to the recently publicized targeting of US Government officials through LinkedIn.[10]

[10] U.S. Army Cyber Command, *Army Cyber Fact Sheet: LinkedIn Scams* (September 26, 2019), *available at* https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1972156/army-cyber-fact-sheet-linkedin-scams.

C. Cybersecurity Program

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, largest cities, most critical military bases, countless defense contractors and small businesses.

At the Companies, everyone plays a part in cybersecurity. The cybersecurity program is led by the Cybersecurity department. The mitigations discussed in this chapter focus on those control activities performed or supported directly by the Cybersecurity department as a shared service for SDG&E, SoCalGas, and Sempra Energy. The Cybersecurity department manages cybersecurity risks across the enterprise, including information technology and operational technology.

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

III. RISK ASSESSMENT

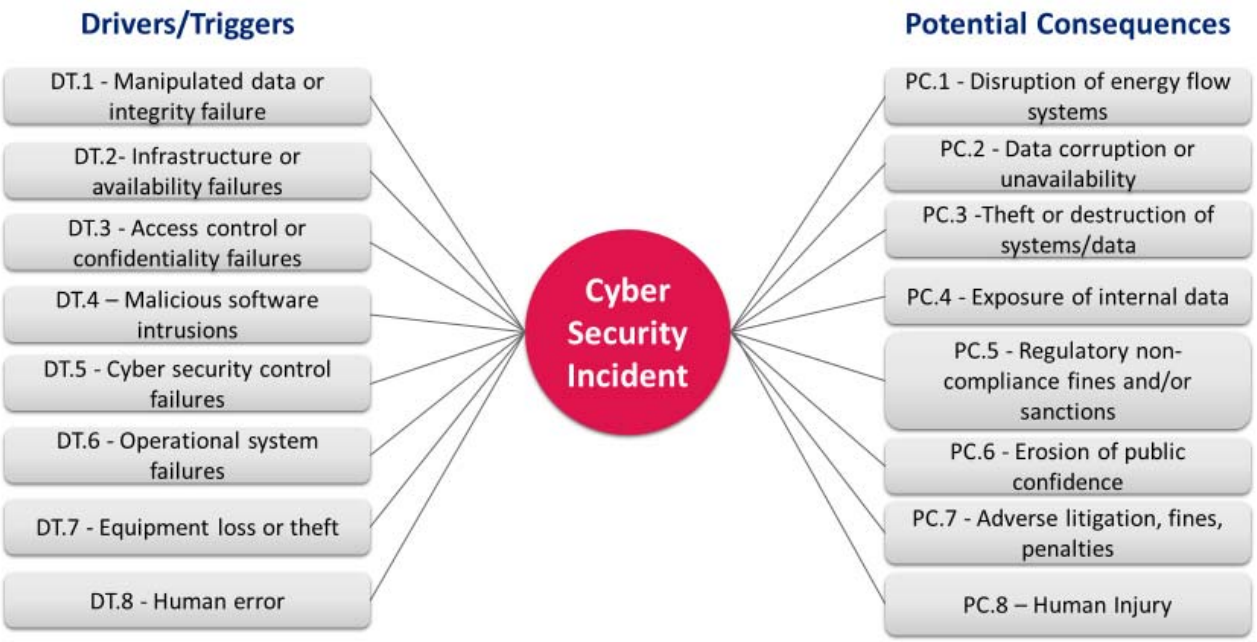
In accordance with the SA Decision,[11] this section describes the Risk Bow Tie, possible Drivers/Triggers, and Potential Consequences of the Cybersecurity risk.

A. Risk Bow Tie

The Risk Bow Tie shown in Figure 1, below, is a commonly-used tool for risk analysis. The left side of the Risk Bow Tie illustrates drivers that lead to a risk event and the right side shows the potential consequences of a risk event. The Companies applied this framework to identify and summarize the information provided above. A mapping of each Control to the element(s) of the Risk Bow Tie addressed is provided in Appendix A.

[11] D.18-12-014 at 33 and Attachment A, A-11 ("Bow Tie").

Figure 1: Risk Bow Tie



B. Asset Groups or Systems Subject to the Risk

The SA Decision[12] directs the utilities to endeavor to identify all asset groups or systems subject to the risk. The Cybersecurity risk is a "cross-cutting" risk impacting all of the Companies' electric and gas operations assets, infrastructure, and systems, including: information technology (IT) perimeter, the IT internal systems, sensitive data within the IT systems, legacy technology infrastructure, and operational technology.

C. Risk Event Associated with the Risk

The SA Decision[13] instructs the utilities to include a Risk Bow Tie illustration for each risk included in RAMP. As illustrated in the above Risk Bow Tie, the risk event (center of the bow tie) is a Cybersecurity event that results in any of the Potential Consequences listed on the right. The Drivers/Triggers that may contribute to this risk event are further described in the section below. There are many possible ways in which a cybersecurity event can occur. The

[12] *Id.* at Attachment A, A-11 ("Definition of Risk Events and Tranches").

[13] *Id.* at Attachment A, A-11 ("Bow Tie").

scenario below represents a situation that could happen, within a reasonable timeframe, and lead to a relatively significant adverse outcome.

Possible scenario: A malicious cyber attacker successfully accesses Company information or technology assets, which results in disruption in energy delivery, creates an unsafe condition with safety impacts, damages financial or other operational systems, and/or exposes customer data.

D. Potential Drivers/Triggers[14]

The SA Decision[15] instructs the utility to identify which element(s) of the associated bow tie each mitigation addresses. When performing the risk assessment for Cybersecurity, the Companies identified potential leading indicators, referred to as drivers. 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**: Refers to 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.
- **DT.4 - Malicious software intrusions**: Describes any malicious program or code that is harmful to systems. 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.

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

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

- **DT.5 - Cybersecurity control failures**: Refers to 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 failures**: A system failure occurring due a cybersecurity event/incident, causing the system to freeze, reboot, or stop functioning altogether.
- **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):** Refers to an accidental cybersecurity event/incident conducted by a human.

E. Potential Consequences

There are several potential worst-case scenarios that the Companies consider. However, as noted earlier, we are intentionally not sharing the details of these scenarios to avoid informing adversaries. 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**: Refers to a power outage, or failure of gas distribution, where there is the loss of electrical power, or natural gas supply, to an end user. Energy delivery failures are particularly critical at sites where the environment and public safety are at risk.
- **PC.2 - Data corruption or unavailability**: A situation where data is made unavailable or modified via failures in storage, transmission, processing, or a cybersecurity incident (*e.g.*, "Ransomware" attack).
- **PC.3 - Theft or destruction of systems/data**: A situation where data is accidentally or maliciously destroyed (made unavailable) or stolen causing an impact to business operations, reputation and/or financial harm.
- **PC.4 - Exposure of sensitive Company and customer data**: Exposure of sensitive Company and customer data can be a significant cybersecurity

incident to an organization with consequences that can include loss of customer confidence, public trust, financial penalties, among others.

- **PC.5 - Regulatory non-compliance fines and/or sanctions:** The risk of a regulatory compliance failure which results in potential penalties/fines or sanctions.
- **PC.6 - Erosion of public confidence:** Refers to a cybersecurity event/ incident causing a potential loss to financial capital, social capital and/or market share resulting from damages to a firm's reputation.
- **PC.7 - Adverse litigation:** Refers to Litigation risk, which is the possibility that legal action will be taken because of an individual's or corporation's actions, inaction, products, services or other events. Corporations generally employ some type of litigation risk analysis and management to identify key areas where the litigation risk is high, and thereby take appropriate measures to limit or eliminate those risks**.**
- **PC.8 – Human injury:** Refers to physical trauma to the body.

These Potential Consequences were used in the scoring of the Companies' Cybersecurity Risk during the development of the 2018 Enterprise Risk Registry.

IV. RISK QUANTIFICATION

The SA Decision[16] sets minimum requirements for risk and mitigation analysis in RAMP, including enhancements to the Interim Decision 16-08-018.[17] The Companies used the guidelines in the SA Decision as a basis for analyzing and quantifying risks, as shown below. Chapter RAMP-C of this RAMP Report explains the Risk Quantitative Framework which underlies this Chapter, including how the Pre-Mitigation Risk Score, Likelihood of Risk Event (LoRE), and Consequence of Risk Event (CoRE) are calculated.

[16] *Id.* at Attachment A.

[17] *Id.* at 2-3.

Table 3: Pre-Mitigation Analysis Risk Quantification Scores[18]

Cyber Security	Low Alternative	Single Point	High Alternative
Pre-Mitigation Risk Score	897	**920**	958
LoRE	**0.02**		
CoRE	44873	**46018**	47925

A. Risk Scope & Methodology

The SA Decision requires a pre- and post-mitigation risk calculation.[19] The below section provides an overview of the scope and methodologies applied for the purpose of risk quantification.

Table 4: Risk Quantification Scope

In-Scope for purposes of risk quantification:	Major cybersecurity incident on the SCADA system[20] which results in disruptions to electric or gas operations.
Out-of-Scope for purposes of risk quantification:	Disruption to Company operations (*e.g.,* HR, payroll, billing), reputation, or disclosure of sensitive customer or Company data.

Given the emerging and evolving nature of cyber 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.

---

[18] The term "pre-mitigation analysis," in the language of the SA 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.

[19] D.18-12-014 at Attachment A, A-11 ("Calculation of Risk").

[20] SCADA is an acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real time data.

Several data points and sources were used to help the Companies' subject matter experts (SME) estimate the likelihood of this event. According to the "Lloyd's Report – The Insurance Implications of a Cyber Attack on the US Power Grid," there have been 15 suspected cyber-attacks or events on the US electric grid from 2000 to 2015.[21] The estimate of the likelihood of the scenario based on that report is in the order of 2% (1 in 50 years). In addition, the Accenture, "Cost of Cyber Crime Study,"[22] indicates a rapidly evolving risk increasing at an annual rate of 27%.[23] Given this information, the Companies' SMEs provide a likelihood of 2% for the cyber risk or 1:50 years.

To determine the Potential Consequences, the Companies, including SMEs from Cybersecurity, electric operations, and gas operations, evaluated relevant industry event scenarios to determine a credible worst-case scenario of a cyberattack at the Companies. The scenarios evaluated account for the potential unavailability of a compromised SCADA system for restoration:

1. Ukraine 2015 and 2016/2018 – 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") to attempt to disable protective relay devices through a denial of service (DoS) attack. Though 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.
2. 2011 South West Outage – In 2011, a maintenance procedure in Yuma, Arizona caused a cascade of power failures across the Southwest resulting in widespread impact to SDG&E's service territory. As the failure spread, grid operators were

---

[21] Lloyd's, *Emerging Risk Report – 2015, Business Blackout, The Insurance Implications of a Cyber Attack on the US Power Grid* (May 2015) at 53, *available at* https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout.

[22] Accenture, *2017 Cost of Cyber Crime Study, Insights on the Security Investments That Make A Difference*, *available at* https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.

[23] *Id.* at 4.

unaware of many rapid-fire events outside their territories. Electrical service was restored to most SDG&E customers within 12 hours.

3. 2003 North East Outage – The biggest blackout in North America occurred in 2003. High voltage power lines came into contact with vegetation, and a combination of human error and equipment failures resulted in outages for 50 million people.

4. Lloyds Scenarios (Scenario 1) - A report produced by Lloyd's and the University of Cambridge considered the impact of a hypothetical cyber-attack. In the scenario, malware infects generation control rooms in 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.

B. Sources of Input

The SA Decision[24] directs the utility to identify Potential Consequences of a Risk Event using available and appropriate data. The below provides a listing of the inputs utilized as part of this assessment.

1. Richards, Kevin, "Accenture Report the Cost of Cyber Crime," dated 2017;
2. Maynard, Trevor, "Lloyd's Report the Insurance Implications of a Cyber Attack on the US Grid," dated May 2015; and
3. Slowick, Joe, "Dragos Inc CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," August 16, 2019.

V. RISK MITIGATION PLAN

The SA Decision requires a utility to "clearly and transparently explain its rationale for selecting mitigations for each risk and for its selection of its overall portfolio of mitigations."[25] This section describes the Companies' Risk Mitigation Plan by each selected Control for this risk, including the rationale supporting each selected Control.

---

[24] D.18-12-014 at Attachment A, A-8 – A-9 ("Identification of the Frequency of the Risk Event").

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

The Cybersecurity Risk Mitigation Plan discussed below includes the five operational categories introduced in Section I above. The Risk Mitigation Plan includes Controls and Mitigations that are expected to continue for the period of the Companies' TY 2022 GRC cycle.[26] The Controls (*i.e.*, those with a "C" identifier below) are those activities that were in place as of 2018, most of which have been developed over many years, to address this risk and include work to comply with laws that were in effect at that time. In addition, the Companies have considered the evolving threat and regulatory landscape in the design of its plan. 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 Presented Portfolio is designed to provide adequate risk reduction to offset the projected cyber risk increase to maintain this risk at a manageable level.

A. SDG&E-10-C1/SCG-9-C1: Perimeter Defenses

The Perimeter Defenses category includes activities that the Companies take to protect the perimeter of its information technology systems. 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 further impacts and/or a full breach.

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.

Examples of the Companies' existing Perimeter Defenses include:

- Web application firewalls;

[26] *Id.* at 16-17 and 33. A "Control" is defined as a "[c]urrently established measure that is modifying risk." 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."

- Access management at the perimeter;
- Penetration testing of our perimeter to regularly challenge our defense capabilities;
- Multi-factor authentication to enhance user access controls;
- Enhanced firewalls, intrusion detection and prevention technologies;
- Email security gateway to enhance email system security; and
- Web content filter to enhance safer web site browsing/access.

B. SDG&E-10-C2/SCG-9-C2: Internal Defenses

Program activities in the Internal Defenses category are designed to detect and prevent unauthorized users, those misusing authorized credentials, and malicious software (*i.e.*, malware) from propagating inside of the perimeter. As another layer of defense-in-depth, the activities within this category include investments that will directly reduce the risk to internal assets and information. This control focuses on:

- Preventing unauthorized access to technology, systems and/or information;
- Validating that only authorized users are using a profile or credentials associated with that user (authorized employee);
- Analysis of potentially unusual and/or malicious activities;
- Automating threat detection and response activities to decrease cybersecurity risk;
- Improve ability to meet compliance requirements (*e.g.*, CCPA, NERC CIP, etc.);[27]
- Enhancing cloud security (*i.e.*, as an extension of the internal Company system); and
- Network security monitoring.

[27] California Consumer Privacy Act, North American Electric Reliability Corporation Critical Infrastructure Protection standards.

C. SDG&E-10-C3/SCG-9-C3: Sensitive Data Protection

Sensitive data protection is a core component of the Companies' defense-in-depth strategy for cybersecurity. The Sensitive Data Protection activities outlined below enhance technology to reduce the risk of unauthorized access. 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:

- Automatically scan assets to identify location of sensitive data;
- Identify the movement, copying, or dissemination of data from central and mobile technology systems;
- Monitor unauthorized patterns of data movement;
- Multi-factor authentication to enhance user access controls; and
- Data loss prevention to enhance our capabilities in securing information.

D. SDG&E-10-C4/SCG-9-C4: Operational Technology (OT) Cybersecurity

The OT Cybersecurity category focuses on securing the operational technology environments 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. 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 Controls include:

- OT network anomaly detection to identify and prevent potentially malicious network traffic;
- Physical and cybersecurity operations center visibility into operational technology systems;
- Monitoring of endpoint technology devices that control electric and gas assets;

- Visibility into the status and location of all operational technology through asset management;
- Enhanced whitelisting capabilities (to validate that only approved computer programs can run);
- Secure telecommunication network capabilities; and
- Multi-factor authentication to enhance user access controls.

E. SDG&E-10-C5/SCG-9-C5: 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 vulnerable, obsolete technologies. 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/or processes that are no longer effective, and/or potentially could create new vulnerabilities. The controls presented in this section include:

- Technology refreshes, including, but not limited to:
  - Infrastructure;
  - Operating systems;
  - Middleware; and
  - 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.

In addition, there are fundamental, baseline control activities required to support and effectively manage the cybersecurity capabilities listed in the previous sections. These baseline activities referenced in the O&M budget outlook (tables 2 and 3) support the capital investments. Some examples of these baseline controls include, but are not limited to:

- A security policy framework

- Risk management & 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

The combination of existing cybersecurity controls and enhancements will help the Companies keep pace with the rapidly evolving cybersecurity threats.

VI. POST-MITIGATION ANALYSIS

As described in Chapter RAMP-D, the Companies have performed a Step 3 analysis where necessary pursuant to the terms of the SA Decision.

A. Mitigation Tranches and Groupings

The Step 3 analysis provided in the SA Decision[28] instructs the utility to subdivide the group of assets or the system associated with the risk into Tranches. Risk reduction from controls and mitigations and RSEs are determined at the Tranche level. For purposes of the risk analysis, each Tranche is considered to have homogeneous risk profiles (*i.e.*, the same LoRE and CoRE). The Companies' rationale for the determination of Tranches is presented below.

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 category level due to the availability of data, the rapidly

[28] D.18-12-014 at Attachment A, A-11 ("Definition of Risk Events and Tranches").

changing threats and applicable counter measures. Therefore, the level of granularity for quantifying RSE is currently at the operational category 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.

B. Post-Mitigation/Control Analysis Results

For purposes of the post-mitigation and post-control analysis, the Companies looked at historical safety performance results and the improvements year-over-year to calculate an overall risk reduction benefit of performing these activities.[29] The Companies then looked at existing/continuing programs (*i.e.*, Controls), and expect to get similar results (*i.e.*, percentage of risk reduction benefit by continuing the activity). The Companies also accounted for the risk increase that would occur over time if we stopped performing these activities. The specific risk reduction benefit percentages used for each identified control/mitigation is included under each program heading below.

C. SDG&E-10-C1/SCG-9-C1: Perimeter Defenses

1. Description of Risk Reduction Benefits

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 us to understand the number of pathways into or out of the perimeter while simultaneously monitoring the perimeter in real time.

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.

[29] *Id.* at Attachment A, A-12 ("Determination of Post-Mitigation LoRE," "Determination of Post-Mitigation CoRE," "Measurement of Post-Mitigation Risk Score," "Measurement of Risk Reduction Provided by a Mitigation").

2. Elements of the Bow Tie Addressed

SDG&E-10-C1/SCG-9-C1 addresses several Drivers/Triggers and Potential Consequences as outlined above in Figure 1 and in Appendix A. These include: Infrastructure or availability failure (DT.2), Malicious software intrusions (DT.4), Cybersecurity control failures (DT.5), Operational system failures (DT.6), Equipment Loss or Theft (DT.7), Exposure of sensitive Company and customer data (PC.4), Regulatory non-compliance fines and/or sanctions (PC.6).

3. Summary of Results

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0270**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1212.48	**1243.40**	1294.93
	RSE	127.50	**130.75**	136.17

D. SDG&E-10-C2/SCG-9-C2: Internal Defenses

1. Description of Risk Reduction Benefits

Internal Defense controls support the Companies' defense-in-depth strategy, which helps to detect and prevent unauthorized users, those misusing authorized credentials, and malicious software (*i.e.*, malware) from propagating once inside of the perimeter. 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 our ability to identify and respond to threats more quickly. The enhancements to our IT and OT systems' Access Management system will allow us to keep our current risk level steady/static.

2. Elements of the Bow Tie Addressed

SDG&E-10-C2/SCG-9-C2 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), 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 sensitive Company and customer data (PC.4), Regulatory non-compliance fines and/or sanctions (PC.6).

3. Summary of Results

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0256**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1149.48	**1178.79**	1227.64
	RSE	24.49	**25.12**	26.16

E. SDG&E-10-C3/SCG-9-C3: Sensitive Data Protection

1. Description of Risk Reduction Benefits

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 us continue the prudent management of sensitive data.

2. Elements of Bow Tie Addressed

SDG&E-10-C3/SCG-9-C3 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), 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 sensitive Company and customer data (PC.4), Adverse Litigation (PC.5), Regulatory non-compliance fines and/or sanctions (PC.6), Erosion of public confidence (PC.7).

3. Summary of Results

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0228**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1023.47	**1049.57**	1093.07
	RSE	58.13	**59.61**	62.08

F. SDG&E-10-C4/SCG-9-C4: Operational Technology (OT) Cybersecurity

1. Description of Risk Reduction Benefits

The OT environment requires a slightly different approach from IT Cybersecurity. OT activities are intended to reduce the risk of an adversary controlling or disabling the Companies' operational technology. 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 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.

2. Elements of the Bow Tie Addressed

SDG&E-10-C4/SCG-9-C4 addresses several Drivers/Triggers and Potential Consequences as outlined above in Figure 1 and in Appendix A. These include: 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), Adverse litigation (PC.5), Regulatory non-compliance fines and/or sanctions (PC.6), Erosion of public confidence (PC.7).

3. Summary of Results

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0284**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1275.48	**1308.01**	1362.21
	RSE	51.60	**52.92**	55.11

G. SDG&E-10-C5/SCG-9-C5: Obsolete Information Technology (IT) Infrastructure and Application Replacement

1. Description of Risk Reduction Benefits

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.

2. Elements of the Bow Tie Addressed

SDG&E-10-C5/SCG-9-C5 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), Regulatory non-compliance fines and/or sanctions (PC.6).

3. Summary of Results

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0242**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1086.48	**1114.18**	1160.36
	RSE	66.06	**67.74**	70.55

VII. SUMMARY OF RISK MITIGATION PLAN RESULTS

The Companies' Risk Mitigation Plan takes into account recent data and trends related to Cybersecurity, possible labor constraints and the feasibility of mitigations. The Companies have performed RSEs, in compliance with the S-MAP decisions, but ultimate mitigation selection can be influenced by other factors, including technology, planning, resources, compliance requirements, and operational and execution considerations.

The tables below provide a summary of the Risk Mitigation Plan, including controls, associated costs, and RSEs.

The Companies do not account for and track costs by activity, but rather, by cost center and capital budget code. Thus, the costs shown in Tables 5 and 6 below were estimated using assumptions provided by SMEs and available accounting data.

Table 5: SoCalGas Risk Mitigation Plan Summary[30]
(Direct 2018 $000)[31]

ID	Mitigation/Control	Tranche	2018 Baseline Capital[32]	2018 Baseline O&M	2020-2022 Capital[33]	2022 O&M	Total[34]
SCG-9-C1	Perimeter Defenses	T1	5,400	60	6,100 - 7,800	160 - 210	6,300 – 8,000
SCG-9-C2	Internal Defenses	T1	17,000	180	36,000 - 47,000	500 - 630	37,000 – 48,000
SCG-9-C3	Sensitive Data Protection	T1	-	180	5,700 - 7,300	500 - 630	6,200 – 8,000
SCG-9-C4	Operational Technology (OT) Cybersecurity	T1	2,800	150	17,000 - 21,000	410 – 520	17,000 – 22,000
SCG-9-C5	Obsolete IT Infrastructure and Application Replacement	T1	3,300	30	7,400 - 9,500	80 - 110	7,500 – 10,000
TOTAL COST			**29,000**	**600**	**72,000 - 93,000**	**1,700 - 2,000**	**74,000 – 95,000**

[30] Recorded costs and ranges were rounded. Additional cost-related information is provided in workpapers. Costs presented in the workpapers may differ from this table due to rounding.

[31] The figures provided are direct charges and do not include company loaders, with the exception of vacation and sick time. The costs are also in 2018 dollars and have not been escalated to 2019 amounts.

[32] Pursuant to D.14-12-025 and D.16-08-018, the Company provides the 2018 "baseline" capital costs associated with Controls. The 2018 capital amounts are for illustrative purposes only. Because capital programs generally span several years, considering only one year of capital may not represent the entire activity.

[33] The capital presented is the sum of the years 2020, 2021, and 2022 or a three-year total. Years 2020, 2021 and 2022 are the forecast years for SoCalGas' Test Year 2022 GRC Application.

[34] Total = 2020, 2021 and 2022 Capital + 2022 O&M amounts.

Table 6: SDG&E Risk Mitigation Plan Summary[35]
(Direct 2018 $000) [36]

ID	Mitigation/Control	Tranche	2018 Baseline Capital[37]	2018 Baseline O&M	2020-2022 Capital[38]	2022 O&M	Total[39]
SDG&E-10-C1	Perimeter Defenses	T1	-	830	0	1,200 - 1,500	1,200 - 1,500
SDG&E-10-C2	Internal Defenses	T1	-	1,000	0	1,300 - 1,700	1,300 - 1,700
SDG&E-10-C3	Sensitive Data Protection	T1	-	380	0	520- 670	520- 670
SDG&E-10-C4	Operational Technology (OT) Cybersecurity	T1	280	600	8,400 – 11,000	910 - 1,200	9,310 – 12,200
SDG&E-10-C5	Obsolete IT Infrastructure and Application Replacement	T1	1,400	1,000	0	1,300 - 1,700	1,300 - 1,700
TOTAL COST			**1,700**	**3,800**	**8,400 - 11,000**	**5,200 -6,800**	**14,000 – 18,000**

[35] Recorded costs and ranges were rounded. Additional cost-related information is provided in workpapers. Costs presented in the workpapers may differ from this table due to rounding.

[36] The figures provided are direct charges and do not include company loaders, with the exception of vacation and sick time. The costs are also in 2018 dollars and have not been escalated to 2019 amounts.

[37] Pursuant to D.14-12-025 and D.16-08-018, the Company provides the 2018 "baseline" capital costs associated with Controls. The 2018 capital amounts are for illustrative purposes only. Because capital programs generally span several years, considering only one year of capital may not represent the entire activity.

[38] The capital presented is the sum of the years 2020, 2021, and 2022 or a three-year total. Years 2020, 2021 and 2022 are the forecast years for SDG&E's Test Year 2022 GRC Application.

[39] Total = 2020, 2021 and 2022 Capital + 2022 O&M amounts.

It is important to note that the Companies are identifying potential ranges of costs in this Risk Mitigation Plan and are not requesting funding herein. The Companies will integrate the results of this proceeding, including requesting approval of the activities and associated funding, in the next GRC.

VIII. ALTERNATIVE ANALYSIS

Pursuant to D.14-12-025 and D.16-08-018, the Companies considered alternatives to the Risk Mitigation Plan for the Cybersecurity risk. Typically, analysis of alternatives occurs when implementing activities to obtain the best result or product for the cost.

The alternatives analysis for this Risk Mitigation Plan also considered modifications to the Presented Portfolio and constraints, such as budget and resources. The Companies considered two Alternative Portfolios to the Presented Portfolio identified above as it developed the Risk Mitigation Plan to address the Companies' Cybersecurity risk. Alternatives were analyzed in the context of risk-spend efficiency, outlined in the tables below, and considered as portfolios rather than individual mitigations.

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

1. Presented Portfolio,
2. Alternative 1, and
3. Alternative 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:

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

- Extent to which each project addresses recommendations from CSC 20,[40] ICS-CERT,[41] and other frameworks;
- Extent to which each project addresses threats to cybersecurity of high impact and likelihood; and
- Effectiveness in mitigating a credible attack impacting safety.

After each project was tagged as High/Medium/Low, the following three portfolios were developed: Presented Portfolio, Alternative Portfolio 1 and Alternative Portfolio 2.

A. Presented Portfolio

The Companies' Presented Portfolio (*i.e.*, the Risk Mitigation Plan as described in Sections V and VI, above) includes a mix of "high" impact and "medium" impact projects. The identified high-impact and medium-impact projects were grouped into the five categories 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 post-mitigation analysis demonstrates that the Companies' Presented Portfolio 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. Company SMEs estimated that the Presented Portfolio will have an effectiveness proportional to the growth rate of the risk of cybersecurity threats, hence funding at this level will maintain the risk at a manageable level.

---

[40] 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.

[41] ICS-CERT: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT 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 categories described above. The post-mitigation analysis demonstrates that the Companies' Alternative Portfolio 1, comprising only high-impact projects, is estimated to have a lower RSE than the Presented Portfolio 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, as estimated by the Companies; hence, if we fund at this level, the cyber risk will increase. The post-mitigation 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' Presented Portfolio provided in Sections V and VI.

1. Alternative Portfolio 1 – C1 (High-impact Perimeter Defenses)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0256**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1149.48	**1178.79**	1227.64
	RSE	122.26	**125.37**	130.57

2. Alternative Portfolio 1 – C2 (High-impact Internal Defenses)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0228**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1023.47	**1049.57**	1093.07
	RSE	15.53	**15.93**	16.59

3. Alternative Portfolio 1 – C3 (High-impact Sensitive Data Protection)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0214**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	960.47	**984.96**	1025.78
	RSE	35.83	**36.74**	38.26

4. Alternative Portfolio 1 – C4 (High-impact OT Cybersecurity)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0276**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1237.68	**1269.24**	1321.84
	RSE	52.69	**54.03**	56.27

5. Alternative Portfolio 1 – C5 (High-impact Obsolete IT Infrastructure and Application Replacement)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0238**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1067.57	**1094.80**	1140.17
	RSE	65.03	**66.69**	69.46

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' Presented Portfolio includes high- and medium-impact projects, and Alternative Portfolio 1 includes only high-

impact projects, this Alternative Portfolio 2 presents all projects that the Companies have currently identified. Alternative Portfolio 2 has the highest cost, and the most risk reduction. Alternative Portfolio 2 has an RSE lower than the Presented Portfolio since the additional projects in the portfolio (the low-impact projects beyond those included in the Presented Portfolio) 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)

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0277**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1243.98	**1275.70**	1328.57
	RSE	123.40	**126.55**	131.80

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

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0262**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1174.68	**1204.63**	1254.56
	RSE	24.32	**24.94**	25.97

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

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0228**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1023.47	**1049.57**	1093.07
	RSE	58.13	**59.61**	62.08

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

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0284**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1275.48	**1308.01**	1362.21
	RSE	51.60	**52.92**	55.11

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

		Low Alternative	Single Point	High Alternative
Pre-Mitigation	**LoRE**		**0.020**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	897.47	**920.35**	958.50
Post-Mitigation	**LoRE**		**0.0242**	
	CoRE	44873.42	**46017.68**	47924.79
	Risk Score	1086.48	**1114.18**	1160.36
	RSE	66.06	**67.74**	70.55

APPENDIX A: SUMMARY OF ELEMENTS OF RISK BOW TIE ADDRESSED

Control ID	Control Name	Driver(s), Trigger(s) & Potential Consequences Addressed
SDG&E-10-C1 SCG-9-C1	Perimeter Defenses	DT.2, DT.4, DT.5, DT.6, DT.7 PC.4, PC.6
SDG&E-10-C2 SCG-9-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
SDG&E-10-C3 SCG-9-C3	Sensitive Data Protection	DT.1, DT.3, DT.5, DT.8, PC.2, PC.3, PC.4, PC.5, PC.6, PC.7
SDG&E-10-C4 SCG-9-C4	Operational Technology (OT) Cybersecurity	DT.1, DT.2, DT.3, DT.4, DT.5, DT.6, DT.8 PC.1, PC.2, PC.5, PC.6, PC.7
SDG&E-10-C5 SCG-9-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