Risk Assessment Mitigation Phase
Risk Mitigation Plan
Physical Security of Critical Gas Infrastructure
(Chapter SCG-6)

November 30, 2016

310271

SoCalGas
A Sempra Energy utility

TABLE OF CONTENTS

Executive Summary

The Physical Security of Critical Infrastructure (Physical Security) risk relates to the damage to critical gas infrastructure that can result from intentional acts.

To assess this risk, SoCalGas first identified a reasonable worst case scenario, and scored the scenario against five residual impact categories (e.g., Health, Safety, Environmental; Operational & Reliability, etc., discussed in Section 4). Then, SoCalGas considered as a baseline, the SoCalGas mitigation in place for in 2015 for Physical Security and estimated the costs (costs are discussed in Section 7). SoCalGas identified the following controls as of 2015:

1. Physical Security Systems and Contract Security: including physical security systems and contract security (e.g., security guards);
2. Operational Resiliency; and,
3. Planning, Awareness, and Incident Management: including, for example, Critical Asset Security Team, investigations, risk management program, training, etc.

These controls focus on safety-related impacts (e.g., Health, Safety, and Environment) per guidance provided by the Commission in Decision 16-08-018 as well as controls and mitigations that may address reliability.

Based on the foregoing assessment, SoCalGas proposed future mitigations. For Physical Security, SoCalGas proposed to continue the three control categories, identified above, but included the following enhancements or additional mitigations within these two control categories:

1. Physical Security Systems and Contract Security
    - Install or upgrade access control and detection capabilities
    - Add security guards to new locations and comply with new laws enacted since the baseline evaluation that increase labor costs
2. Planning, Awareness, and Incident Management: additional personnel in risk management and corporate security areas.

Next, SoCalGas developed the risk spend efficiency. The risk spend efficiency is a new tool that SoCalGas developed to attempt to quantify how the proposed mitigations will incrementally reduce risk. The RSE was determined using the proposed mitigations and resulted prioritizing mitigation activities.

Finally, SoCalGas considered two alternatives to the proposed mitigations, and summarizes the reasons that the two alternatives were not selected as a proposed mitigation.

Risk: Physical Security of Critical Infrastructure

1 Purpose

The purpose of this chapter is to present the mitigation plan of Southern California Gas Company (SoCalGas or Company) for the risk of damage to "critical" gas infrastructure. This risk involves damage caused by intentional acts, including but not limited to theft, robbery, burglary, vandalism, disgruntled individuals or groups, terrorism, trespassing, etc., which results in a gas leak, fire, explosion, and/or outages.

This risk is a product of SoCalGas' September 2015 annual risk registry assessment cycle. Any events that occurred after that time were not considered in determining the 2015 risk assessment, in preparation for this Report. While 2015 is used as a base year for mitigation planning, risk management has been occurring, successfully, for many years within the Company. SoCalGas and San Diego Gas & Electric Company (SDG&E) (collectively, the Utilities) take compliance and managing risks seriously, as can be seen by the number of actions taken to mitigate each risk. This is the first time, however, that the utilities have presented a Risk Assessment Mitigation Phase (RAMP) Report, so it is important to consider the data presented in this plan in that context. The baseline mitigations are determined based on the relative expenditures during 2015; however, the utilities do not currently track expenditures in this way, so the baseline amounts are the best effort of each utility to benchmark both capital and operations and maintenance (O&M) costs during that year. The level of precision in process and outcomes is expected to evolve through work with the California Public Utilities Commission (Commission or CPUC) and other stakeholders over the next several General Rate Case (GRC) cycles.

The Commission has ordered that RAMP be focused on safety related risks and mitigating those risks.[1] In many risks, safety and reliability are inherently related and cannot be separated, and the mitigations reflect that fact. Compliance with laws and regulations is also inherently tied to safety and the utilities take those activities very seriously. In all cases, the 2015 baseline mitigations include activities and amounts necessary to comply with the laws in place at that time. Laws rapidly evolve, however, so the RAMP baseline has not taken into account any new laws that have been passed since September 2015. Some proposed mitigations, however, do take into account those new laws.

The purpose of RAMP is not to request funding. Any funding requests will be made in the GRC. The forecasts for mitigation are not for funding purposes, but are rather to provide a range for the future GRC filing. This range will be refined with supporting testimony in the GRC. Although some risks have overlapping costs, the utilities have made efforts to identify those costs.

[1] D. 14-12-025 at p. 31.

2 Background

The risk assessment provided herein focuses on *critical* gas infrastructure[2] in accordance with Transportation Security Administration (TSA) guidelines.[3] The TSA guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators.

For this chapter, SoCalGas only addresses intentional acts that may impact "critical" gas infrastructure. Accordingly, any gas infrastructure that does not meet the TSA's criteria of "critical" is not included and this chapter does not address incidents that are considered to be unintentional such as a vehicular accident rupturing a gas pipeline.

In compliance with these guidelines, SoCalGas has instituted security enhancements or upgrades to infrastructure which have improved access control, intrusion detection, and interdiction capabilities to deter, detect, delay, or mitigate physical risk events at SoCalGas facilities. Depending on the facility, SoCalGas completed several security upgrades, including but not limited to improvements to access, detection, and interdiction.

3 Risk Information

As stated in the testimony of Jorge M. DaSilva in the Safety Model Assessment Proceeding (S-MAP) Application (A.) 15-05-004, "SoCalGas is moving towards a more structured approach to classifying risks and mitigations through the development of its new risk taxonomy. The purpose of the risk taxonomy is to define a rational, logical and common framework that can be used to understand, analyze and categorize risks." The Enterprise Risk Management (ERM) process and lexicon that SoCalGas has put in place was built on the internationally-accepted IS0 31000 risk management standard. In the application and evolution of this process, the Company is committed to increasing the use of quantification within its evaluation and prioritization of risks. This includes identifying leading indicators of risk. Sections 3 – 9 of this chapter describe the key outputs of the ERM process and resultant risk mitigations.

In accordance with the ERM process, this section describes the risk classification, possible drivers and potential consequences of the Physical Security of Critical Infrastructure.

---

[2] Critical gas infrastructure information is confidential and protected from disclosure. *See e.g.,* 18 CFR §388.113(c); FERC Orders 630, 643, 649, 662, 683, and 702 (defining CEII); 6 U.S.C. §§131(3), 133(a)(1)(E); 6 CFR §§ 29.2(b), 29.8 (defining CII and restricting its disclosure); Gov't Code § 6254(e) & (ab) (Plant production data, and similar information relating to utility systems development and "Critical infrastructure information" may be exempt from disclosure under the Public Records Act); FAST Act (Critical Electric Infrastructure Security) Amended December 4, 2015.

[3] TSA, "Pipeline Security Guidelines," April 2011.

3.1 Risk Classification

Consistent with the taxonomy presented by SoCalGas and SDG&E in A.15-05-004, SoCalGas classifies this risk as a gas, operational risk as shown in Table 1.

Table 1: Risk Classification per Taxonomy

Risk Type	Asset/Function Category	Asset/Function Type
OPERATIONAL	GAS	VARIOUS

3.2 Potential Drivers[4]

When performing the risk assessment for Physical Security of Critical Infrastructure, SoCalGas identified potential indicators of risk, referred to as drivers. These include, but are not limited to:

1. **Intentional Damage** – a purposeful act via theft, vandalism, disgruntled employees, terrorism, trespassing that leads to service interruptions or disruption of operations to a critical gas transportation/delivery facility.
2. **Human Error** – an error that occurs due to someone not doing something correctly which leads to the realization of the risk.
3. **Process Failure** – a failure of programs/procedures that are intended to prevent the risk from occurring and control the consequence of the risk if it occurs.
4. **System Failure** – a failure of security systems that are intended to prevent the risk from occurring.

Table 2 maps the specific drivers of the Physical Security of Critical Infrastructure risk to SoCalGas' risk taxonomy.

Table 2: Operational Risk Drivers

Driver Category	Physical Security of Critical Infrastructure Driver(s)
Asset Failure	• System Failure
Asset-Related IT Failure	• System Failure
Employee Incident	• Intentional Damage • Human Error • Process Failure
Contractor Incident	• Intentional Damage • Human Error

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

	• Process Failure
Public Incident	• Intentional Damage
Force of Nature	Not applicable

In addition to the above drivers, other potential circumstances may contribute to the risk of Physical Security, including intentional attacks as a result of: extremist ideologies, criminal acts, personal issues or conflict, mental health issues. The list of drivers and potential circumstances are not intended to be a comprehensive list as Physical Security incidents may vary from one incident to another.

3.3 Potential Consequences

If one of the drivers listed above were to occur resulting in a Physical Security-related event, the potential consequences may include:

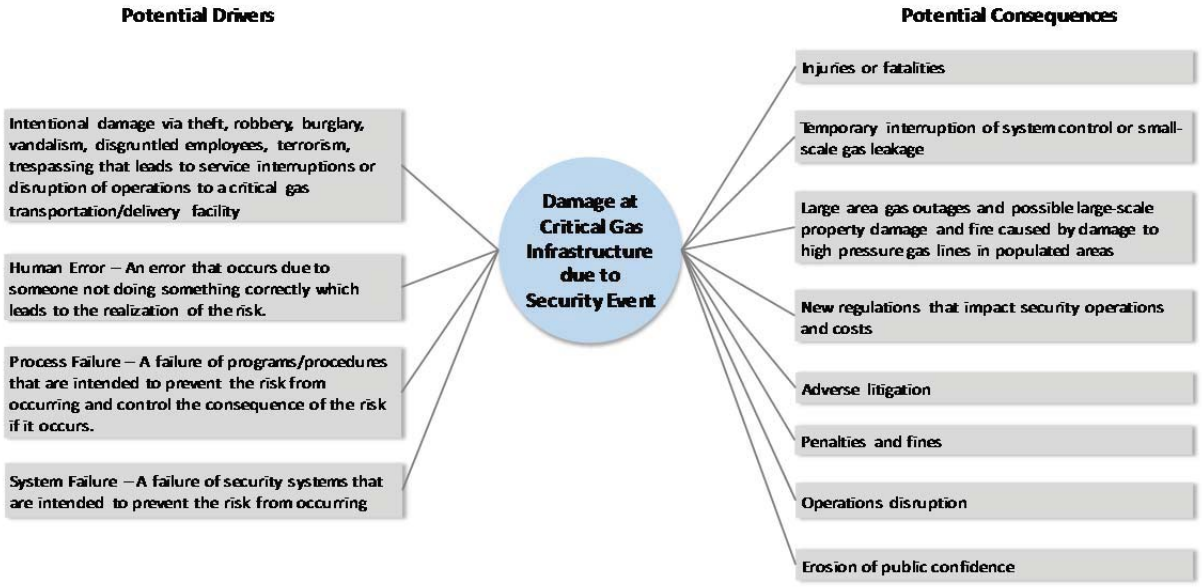
- Injuries or fatalities;
- Temporary interruption of system control or small-scale gas leakage;
- Large area gas outages and possible large-scale property damage and fire caused by damage to high pressure gas lines in populated areas;
- New regulations that impact security operations and costs;
- Adverse litigation and resulting financial consequences;
- Erosion of public confidence; and
- Operations disruption.

These potential consequences were used in the scoring of Physical Security that occurred during SoCalGas' risk registry process. Section 4 contains the risk scoring discussion.

3.4 Risk Bow Tie

The risk "bow tie," shown below, is a commonly-used tool for risk analysis. The left side of the bow tie illustrates potential drivers that may lead to a risk event and the right side shows the potential consequences of a risk event. SoCalGas applied this framework to identify and summarize the information provided in Sections 3.2 and 3.3, above.

Figure 1: Risk Bow Tie



4 Risk Score

The SoCalGas and SDG&E ERM organization facilitated the 2015 risk registry process, which resulted in the inclusion of Physical Security as a potential enterprise risks. During the development of the risk register, subject matter experts (SMEs) assigned a score to this risk, based on empirical data, to the extent it is available and/or using their expertise, and followed the process outlined in this section.

4.1 Risk Scenario – Reasonable Worst Case

Critical infrastructure damage could occur in varied ways. For purposes of scoring this risk, SMEs applied a reasonable worst case scenario to assess the impact and frequency. The scenario represented a hypothetical situation that could happen, within a reasonable timeframe, and could lead to a relatively significant adverse outcome. These types of scenarios are sometimes referred to as low frequency, high consequence events. The SMEs used the reasonable worst case scenario to develop a risk score and the scenario selected to assess the Physical Security risk is:

- A terrorist group uses explosives to rupture major transmission lines, which results in a fire. Employees and members of the public may sustain injuries. This also may result in severe

disruption to the gas supply with potentially widespread curtailments of both core and noncore customers.

Note that the following narrative and scores are based on this scenario; they do not address all consequences that can happen if the risk occurs.

4.2 2015 Risk Assessment

Using this scenario, subject matter experts then evaluated the frequency of occurrence and potential impact of the risk using SoCalGas' 7X7 Risk Evaluation Framework (REF). The framework (also called a matrix) includes criteria to assess levels of impact ranging from Insignificant to Catastrophic and levels of frequency ranging from Remote to Common. The 7X7 framework includes one or more criteria to distinguish one level from another. The Commission adopted the REF as a valid method to assess risks for purposes of this RAMP. Using the levels defined in the REF, the SMEs applied empirical data to the extent it is available and/or their expertise to determine a score for each of four residual impact areas and the frequency of occurrence of the risk.

Table 3 provides a summary of the Physical Security risk score in 2015. This risk has a score of 4 or above in the Health, Safety, and Environmental impact area and, therefore, SoCalGas included this risk in the RAMP. These are residual scores because they reflect the risk remaining after existing controls are in place. For additional information regarding the REF, please refer to the RAMP Risk Management Framework chapter within this Report.

Table 3: Risk Score

Residual Impact				Frequency	Total
Health, Safety, Environmental (40%)	Operational & Reliability (20%)	Regulatory, Legal, Compliance (20%)	Financial (20%)		
5	6	4	4	3	23,107

4.3 Explanation of Health, Safety, and Environmental Impact Score

Considering the reasonable worst case scenario, SoCalGas assumed that terrorists willing to carry out this type of attack may also harm employees onsite or nearby. In addition, in this scenario, SoCalGas assumed the explosive devices could harm workers or neighbors within the area if they were situated near the explosion or fire. This rating also considers the potential disruption to public safety operations and health and human services that may rely on natural gas operations. Accordingly, SoCalGas scored Physical Security a 5 (extensive) in the Health, Safety, and Environmental impact area.

4.4 Explanation of Other Impact Scores

Based on the selected reasonable worst case risk scenario, SoCalGas scored the other residual impact areas as follows:

- **Operational and Reliability:** SoCalGas rated Physical Security a 6 (severe) in the Operational and Reliability impact area. The criticality of gas facilities can vary the impact of the incident

and outage type. Accordingly, in applying the reasonable worst case scenario, SoCalGas assumed that a significant loss will occur in which all major pipelines at a single facility are significantly damaged or impacted by a terrorist event and the reliability of gas service to the region will be compromised, resulting in curtailments of both core and non-core customers.

- **Regulatory, Legal and Compliance:** SoCalGas scored the Regulatory, Legal, and Compliance impact a 4 (major). SoCalGas assigned this score because enhanced regulations may be implemented as a result of the reasonable worst case scenario, similar to the enactment of NERC CIP 14 after Pacific Gas and Electric Company (PG&E)'s Metcalf incident.

- **Financial:** SoCalGas rated Physical Security a 4 (major) in the Financial impact area. The potential costs associated with this type of scenario could range between $10 million and $100 million, which would account for, as a minimum, the following:

    - Temporary, emergency repairs
    - Permitting
    - Material procurement
    - Permanent repairs
    - Pipeline contractors(s)
    - Environmental
    - Inspection
    - Customer Restores
    - Media/Customer Communications
    - Potential litigation
    - Security

4.5 Explanation of Frequency Score

The frequency of terrorist incident penetrating a critical gas facility was considered to be 3 (infrequent), which is defined in accordance with SoCalGas' 7X7 matrix as having the potential to occur every 10-30 years. While attacks against critical gas infrastructure have occurred within the United States, Canada, and Mexico within the last 10 years, the attacks did not cause significant operational disruption and few of the attacks were well planned or successful. However, because there continues to be attacks overseas, terrorist groups could use similar techniques to perform attacks domestically.

5 Baseline Risk Mitigation Plan[5]

As stated above, the Physical Security risk involves damage to critical gas infrastructure resulting from intentional acts. The 2015 baseline mitigations discussed below includes the current evolution of the utilities' risk management of this risk. The baseline mitigations have been developed over many years to address this risk. They include activities to comply with laws that were in effect at that time. SoCalGas' baseline mitigation plan for this risk consists of three controls:

[5] As of 2015, which is the baseline year for purposes of this Report.

(1) Physical Security Systems and Contract Security;

(2) Operational Resiliency; and,

(3) Planning, Awareness, and Incident Management, which includes,

a. Critical Asset Security Team
b. Investigations
c. Risk Management Program
d. Security Awareness Training
e. Law Enforcement Liaison and Trade Groups
f. Utilities Liaison
g. Site Security Reviews
h. Business Resumption Plan
i. Gas Security Plans

SMEs from Corporate Security within Gas Engineering collaborated to identify and document the baseline controls. These controls focus on safety-related impacts[6] (i.e., Health, Safety, and Environment) per guidance provided by the Commission in D.16-08-018[7] as well as controls and mitigations that may address reliability.[8] Accordingly, the controls and mitigations described in this section and in Section 6 address safety-related impacts primarily. Note that the controls and mitigations in the baseline and proposed risk mitigation plans are intended to address various events related to Physical Security and is not limited to the scenario used for the Risk Score.

1. Physical Security Systems and Contract Security

The purpose of physical security is to maintain the safety of employees, contractors, the public, and SoCalGas facilities through the use of systems, personnel and policies and procedures. This includes the maintenance and improvement of safety through the implementation of proactive threat identification and mitigation measures; and more effective access control, detection, and interdiction capabilities. Aligned with this, SoCalGas' physical security mitigation in this chapter includes two activities: physical security systems and contract security (e.g. security guards).

Physical security systems provide protection enhancements to infrastructure to improve access control, intrusion detection, and interdiction capabilities to deter, detect, delay, or prevent undesirable events at Company facilities. The type and extent of security upgrades varies by facility, but several have been completed, including, fences, gates and cameras.

In addition to security systems, SoCalGas employs *contract security* (security guards) to secure and physically protect assets and people. These security guards are located at critical facilities and work

[6] The Baseline and Proposed Risk Mitigation Plans may include mandated, compliance-driven mitigations.
[7] D.16-08-018 at p. 146 states "Overall, the utility should show how it will use its expertise and budget to improve its safety record" and the goal is to "make California safer by identifying the mitigations that can optimize safety."
[8] Reliability typically has an impact on safety. Accordingly, it is difficult to separate reliability and safety.

locations. Company policies and procedures outline physical security procedures, including access control, officer post orders and incident reporting.

2. Operational Resiliency

Operational resiliency relates to the utility's ability to maintain operations or quickly resume operations should one of these facilities be compromised. Operational resiliency at critical sites should allow SoCalGas to maintain safety and reliability even if, e.g., a hypothetical intentional act, such as terrorism, were to occur. SoCalGas addresses operational resiliency by proposing and constructing new or enhanced infrastructure projects and programs.

3. Planning, Awareness, and Incident Management

The Planning, Awareness, and Incident Management mitigation includes projects and programs that largely provide services in an attempt to proactively manage this risk before an event can occur. These mitigations consist of activities such as the Critical Asset Security Team (CAST), training, investigations, Corporate Security's risk management program, Industry Outreach and Planning. SoCalGas provides some examples below.

One example of a Planning, Awareness, and Incident Management mitigation is the CAST. CAST is composed of personnel from multiple business units, including Corporate Security, Engineering, Operations, Legal and Environmental assists with enhancing security at all of SoCalGas' facilities. This cross-functional team was created to assess current security countermeasures across the SoCalGas infrastructure and to make incremental and long-term security recommendations. This team manages the implementation of many of the physical security systems.

Another example is security awareness training. SoCalGas offers a number of training opportunities to employees to increase awareness regarding the identification and response to criminal activity. Security awareness training focuses on identifying threats and suspicious activity, responding to threats, and proper reporting protocols. Training is also provided to external public safety representatives to increase awareness of SoCalGas facilities, infrastructure, and operations. SoCalGas also engages with other external entities including participation in trade groups, security committees, or other working groups with utilities. This outreach assists with the sharing of information regarding security incidents, response, and prevention. It is also an important tool to assist with benchmarking certain topics related to Physical Security.

6 Proposed Risk Mitigation Plan

The 2015 baseline mitigations discussed in Section 5 will continue to be performed in the Proposed Risk Mitigation Plan, in most cases, to maintain the current residual risk level. In addition, the Company is proposing to expand or add the mitigations addressed in this Section.

1. Physical Security Systems and Contract Security

Generally, the baseline controls for Physical Security Systems and Contract Security, described above, will continue. SoCalGas also is proposing similar security projects to enhance protection, such as installing cameras and gates at additional locations. Similarly, the presence of security guards increases protection with the aim of reducing the likelihood of an intentional event.

Regarding security guards, SoCalGas must comply with Senate Bill (SB) 3, which will become effective January 1, 2017. The resulting effects are increases in costs above the standard escalation. In other words, the cost associated with doing business (i.e., employing security guards) has increased, sometimes referred to as non-standard escalation.

2. Operational Resiliency

SoCalGas' operational resiliency activities will include a variety of proposed infrastructure enhancements.

3. Planning, Awareness, and Incident Management

This mitigation consists of expanded and new activities, such as additional personnel in the risk management and corporate security areas. Over the last couple of years, the demand for Corporate Security services has increased as well as regulatory requirements, including the RAMP process, are requiring more detailed security planning and reporting. Given the increase in workload due to increased regulations, additional resources are needed.

7 Summary of Mitigations

Table 4**Error! Reference source not found.** summarizes the 2015 baseline risk mitigation plan, the risk driver(s) addressed by a certain control activity, and the 2015 baseline costs for Physical Security. While control or mitigation activities may address both risk drivers and consequences, risk drivers link directly to the likelihood that a risk event will occur. Thus, risk drivers are specifically highlighted in the summary tables.

SoCalGas does not account for and track costs by activity, but rather, by cost center and capital budget code. So, the costs shown in Table 4 were estimated using assumptions provided by SMEs and available accounting data.

Table 4: Baseline Risk Mitigation Plan[9]
(Direct 2015 $000)[10]

ID	Control	Risk Drivers Addressed	Capital[11]	O&M	Control Total[12]	GRC Total[13]
1	Physical Security Systems	• Intentional Damage • Human Error	$4,480	n/a	$4,480	$4,480
	Contract Security	• Process Failure • System Failure	40	1,670	1,710	1,710
2	Operational Resiliency	• Intentional Damage • Human Error • Process Failure • System Failure	430	n/a	430	430
3	Planning, Awareness, and Incident Management	• Intentional Damage • Human Error • Process Failure • System Failure	n/a	510	510	510
	TOTAL COST		$4,950	$2,180	$7,130	$7,130

***** Includes one or more mandated activities

While all the mitigations and costs presented in Tables 4 and 5 mitigate Physical Security, some of the controls also mitigate other risks presented in this RAMP Report. Specifically, Physical Security Systems, Contract Security, Investigations, the Incident Management System, the Risk Management Program, and Security agent managed by Corporate Security also help mitigate the RAMP risk of Workplace Violence. Accordingly, because there are benefits associated with these activities attributed

[9] Recorded costs were rounded to the nearest $10,000.
[10] The figures provided in Tables 4 and 5 are direct charges and do not include Company overhead loaders, with the exception of vacation and sick. The costs are also in 2015 dollars and have not been escalated to 2016 amounts.
[11] Pursuant to D.14-12-025 and D.16-08-018, the Company is providing the "baseline" costs associated with the current controls, which include the 2015 capital amounts. The 2015 mitigation capital amounts are for illustrative purposes only. Because projects generally span several years, considering only one year of capital may not represent the entire mitigation.
[12] The Control Total column includes GRC items as well as any applicable non-GRC jurisdictional items. Non-GRC items may include those addressed in separate regulatory filings or under the jurisdiction of the Federal Energy Regulatory Commission (FERC).
[13] The GRC Total column shows costs typically presented in a GRC.

to both this risk and Physical Security of Critical Infrastructure, the costs are also presented in both chapters.

Error! Reference source not found. summarizes SoCalGas' proposed mitigation plan, associated projected ranges of estimated O&M expenses for 2019, and projected ranges of estimated capital costs for the years 2017-2019. It is important to note that SoCalGas is identifying potential ranges of costs in this plan, and is not requesting funding approval. SoCalGas will request approval of funding, in its next GRC. There may be non-CPUC jurisdictional mitigation activities addressed in RAMP; any costs associated with these activities will not be carried over to the GRC.

Table 5: Proposed Risk Mitigation Plan[14]
(Direct 2015 $000)

ID	Mitigation	Risk Drivers Addressed	2017 -2019 Capital[15]	2019 O&M	Mitigation Total[16]	GRC Total[17]
1	Physical Security Systems Contract Security	• Intentional Damage • Human Error • Process Failure • System Failure	$10,950 - 13,390 410 - 460	$15 - 20 3,460 - 3,700	$10,970 - 13,410 3,870 - 4,160	$10,970 - 13,410 3,870 - 4,160
2	Operational Resiliency	• Intentional Damage • Human Error • Process Failure • System Failure	12,300 - 17,700	n/a	12,300 - 17,700	12,300 - 17,700
3	Planning, Awareness, and Incident Management	• Intentional Damage • Human Error • Process Failure • System Failure	n/a	660 - 840	660 - 840	660 - 840
	TOTAL COST		$23,660 - 31,550	$4,140 - 4,560	$27,800 - 36,110	$27,800 - 36,110

Status quo is maintained
Expanded or new activity
* Includes one or more mandated activities

[14] Ranges of costs were rounded to the neared $10,000.
[15] The capital presented is the sum of the years 2017, 2018, and 2019 or a three-year total. Years 2017, 2018 and 2019 are the forecast years for SoCalGas' Test Year 2019 GRC Application.
[16] The Mitigation Total column includes GRC items as well as any applicable non-GRC items.
[17] The GRC Total column shows costs typically represented in a GRC.

For Physical Security, the capital forecast was completed using estimated costs for planned security projects. The range provides flexibility as the final scope has not been determined at this time. This estimate is only for physical security systems of critical locations within scope of this risk.

1. Physical Security Systems and Contract Security

   The physical security systems are largely capital projects. While the projects will change (e.g., expansion to additional locations), the projected annual spend is expected to be in line with historical spending. The costs for security guards are based on a five-year average labor cost, along with the cost of complying with SB 3, plus the cost of additional guarded locations. The cost of CAST was estimated using a base-year forecast methodology, as the activity and related costs are not anticipated to change significantly from 2015 levels.

2. Operational Resiliency

   Costs associated with this mitigation were developed by SMEs utilizing their knowledge and experience of what similar projects would cost.

3. Planning, Awareness, and Incident Management

   Many of the mitigations within this grouping used a five-year average (2011-2015) to assist with forecasting of future costs. Some activities that were anticipated to increase used the 2015 base year amounts and added the costs related to incremental activities.

8 Risk Spend Efficiency

Pursuant to D.16-08-018, the utilities are required in this Report to "explicitly include a calculation of risk reduction and a ranking of mitigations based on risk reduction per dollar spent.[18] For the purposes of this Section, Risk Spend Efficiency (RSE) is a ratio developed to quantify and compare the effectiveness of a mitigation at reducing risk to other mitigations for the same risk. It is synonymous with "risk reduction per dollar spent" required in D.16-08-018.[19]

As discussed in greater detail in the RAMP Approach chapter within this Report, to calculate the RSE the Company first quantified the amount of Risk Reduction attributable to a mitigation, then applied the Risk Reduction to the Mitigation Costs (discussed in Section 7). The Company applied this calculation to each of the mitigations or mitigation groupings, then ranked the proposed mitigations in accordance with the RSE result.

[18] D.16-08-018 Ordering Paragraph 8.
[19] D.14-12-025 also refers to this as "estimated mitigation costs in relation to risk mitigation benefits."

8.1 General Overview of Risk Spend Efficiency Methodology

This subsection describes, in general terms, the methods used to quantify the *Risk Reduction*. The quantification process was intended to accommodate the variety of mitigations and accessibility to applicable data pertinent to calculating risk reductions. Importantly, it should be noted that the analysis described in this chapter uses ranges of estimates of costs, risk scores and RSE. Given the newness of RAMP and its associated requirements, the level of precision in the numbers and figures cannot and should not be assumed.

8.1.1 Calculating Risk Reduction

The Company's SMEs followed these steps to calculate the Risk Reduction for each mitigation:

1. **Group mitigations for analysis:** The Company "grouped" the proposed mitigations in one of three ways in order to determine the risk reduction: (1) Use the same groupings as shown in the Proposed Risk Mitigation Plan; (2) Group the mitigations by current controls or future mitigations, and similarities in potential drivers, potential consequences, assets, or dependencies (e.g., purchase of software and training on the software); or (3) Analyze the proposed mitigations as one group (i.e., to cover a range of activities associated with the risk).
2. **Identify mitigation groupings as either current controls or incremental mitigations:** The Company identified the groupings by either current controls, which refer to controls that are already in place, or incremental mitigations, which refer to significantly new or expanded mitigations.
3. **Identify a methodology to quantify the impact of each mitigation grouping:** The Company identified the most pertinent methodology to quantify the potential risk reduction resulting from a mitigation grouping's impact by considering a spectrum of data, including empirical data to the extent available, supplemented with the knowledge and experience of subject matter experts. Sources of data included existing Company data and studies, outputs from data modeling, industry studies, and other third-party data and research.
4. **Calculate the risk reduction (change in the risk score):** Using the methodology in Step 3, the Company determined the change in the risk score by using one of the following two approaches to calculate a Potential Risk Score: (1) for current controls, a Potential Risk Score was calculated that represents the increased risk score if the current control was not in place; (2) for incremental mitigations, a Potential Risk Score was calculated that represents the new risk score if the incremental mitigation is put into place. Next, the Company calculated the risk reduction by taking the residual risk score (See Table 3 in this chapter.) and subtracting the Potential Risk Score. For current controls, the analysis assesses how much the risk might increase (i.e., what the potential risk score would be) if that control was removed.[20] For incremental mitigations, the analysis assesses the anticipated reduction of the risk if the new mitigations are implemented. The change in risk score is the risk reduction attributable to each mitigation.

[20] For purposes of this analysis, the risk event used is the reasonable worst case scenario, described in the Risk Information section of this chapter.

8.1.2 Calculating Risk Spend Efficiency (RSE)

The Company SMEs then incorporated the mitigation costs from Section 7. They multiplied the risk reduction developed in subsection 8.1.1 by the number of years of risk reduction expected to be realized by the expenditure, and divided it by the total expenditure on the mitigation (capital and O&M). The result is a ratio of risk reduction per dollar, or RSE. This number can be used to measure the relative efficiency of each mitigation to another.

Figure shows the RSE calculation.

Figure 2: Formula for Calculating RSE

$$Risk\ Spend\ Efficiency = \frac{Risk\ Reduction * Number\ of\ Years\ of\ Expected\ Risk\ Reduction}{Total\ Mitigation\ Cost\ (in\ thousands)}$$

The RSE is presented in this Report as a range, bounded by the low and high cost estimates shown in Table 5 of this chapter. The resulting RSE scores, in units of risk reduction per dollar, can be used to compare mitigations within a risk, as is shown for each risk in this Report.

8.2 Risk Spend Efficiency Applied to This Risk

SoCalGas analysts used the general approach discussed in Section 8.1, above, in order to assess the RSE for the Gas Physical Security risk. The RAMP Approach Chapter in this Report provides a more detailed example of the calculation used by the Company.

For the purpose of the risk reduction methodology, the risk assessment team combined mitigations into two categories: Physical Security and Operational Resiliency. Physical Security includes physical security systems, guards, and each of the mitigations listed in Planning, Awareness, and Incident Management. The second, Operational Resiliency, consists of various resiliency operations, including AC-injection, withdrawal, and metering debottleneck. Next, SoCalGas further categorized these groups into current or incremental activities. The "Current" category indicates that SoCalGas is currently performing and will continue to perform this activity; "Incremental" refers to a new or significantly expanded activity.

The analysis for Operational Resiliency was based on the assessment of SoCalGas SMEs of potential projects and estimated risk reduction to the overall system. The risk assessment methodology was taken from several Federal-level risk assessment methodologies and included ratings criteria and justifications.

- **Physical Security (current controls)**

The analysis compared the system-wide susceptibility to a physical security attack with and without the baseline mitigations. The frequency adjustment was derived from SoCalGas subject matter experts' physical security risk assessment data. The risk reduction was calculated as the percentage change in the risk assessment score between the current, "with," mitigation assessment score and "without" mitigation assessment score. For the life of the project, the team assumed that long term items, such as fencing, have a life expectancy of 30 years. Shorter term items, such as electronics, have a life of 5 years. The assessment team used a weighted average of ~17 years.

- **Physical Security (incremental mitigations)**

The frequency adjustment was also derived from the SoCalGas subject matter experts' risk assessment spreadsheets. For this mitigation, the analysis compared the current risk assessment score with the risk assessment score after the incremental physical security measures are put in place.

- **Operational Resiliency (incremental mitigations)**

The benefits of this risk were calculated according to the following methodology: Two facilities out of 10 critical facilities will be remedied through the application of the resiliency operations. These operations are estimated to be 40% effective and the effectiveness was weighted for all of the facilities. With the facility weighting, the overall system risk was calculated to be reduced by 5%.

8.3 Risk Spend Efficiency Results

Based on the foregoing analysis, SoCalGas calculated the RSE ratio for each of the proposed mitigation groupings. Following is the ranking of the mitigation groupings from the highest to the lowest efficiency, as indicated by the RSE number:

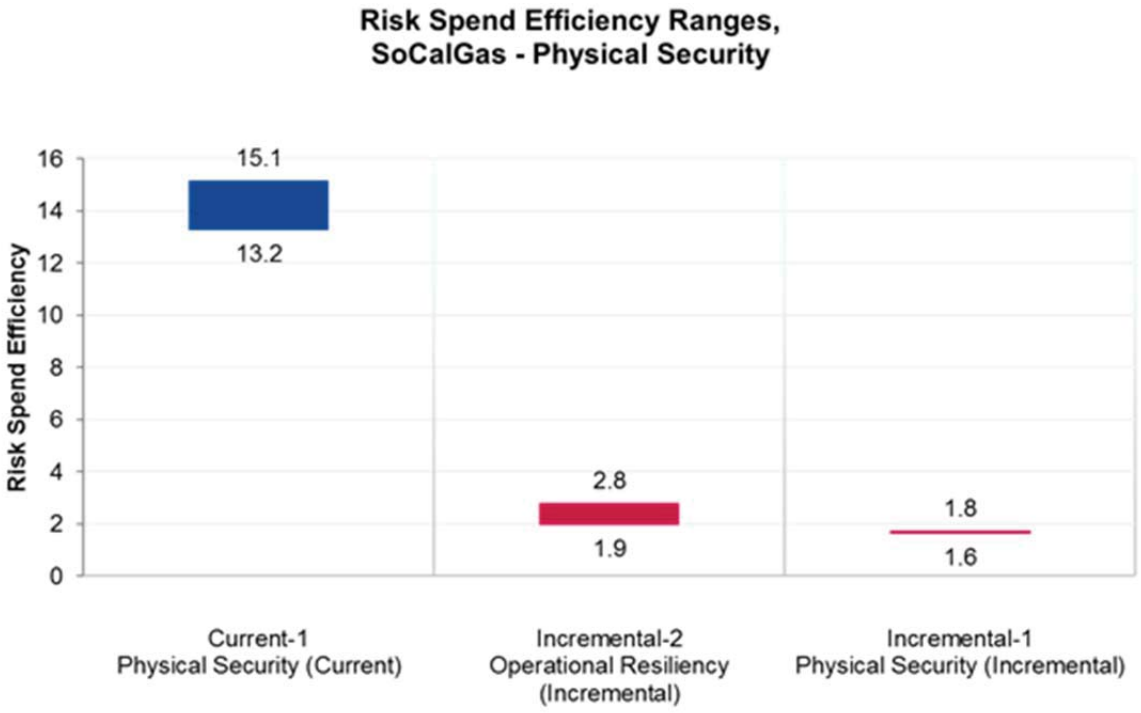
1. Physical Security (current controls)
2. Operational Resiliency (incremental mitigations)
3. Physical Security (incremental mitigations)

Figure displays the range[21] of RSEs for each of the SoCalGas Physical Security risk mitigation groupings, arrayed in descending order.[22] That is, the more efficient mitigations, in terms of risk reduction per spend, are on the left side of the chart.

[21] Based on the low and high cost ranges provided in Table 5 of this chapter.

[22] It is important to note that the risk mitigation prioritization shown in this Report, is not comparable across other risks in this Report.

Figure 3: Risk Spend Efficiency



9 Alternatives Analysis

Alternatives are continually considered as programs are updated. The following represents alternatives for training and for physical security systems that were considered as SoCalGas developed its proposed plan for Physical Security.

9.1 Alternative 1 – Training Changes

SoCalGas considered outsourcing training or developing computer based training as an alternative. Although this alternative may have an increased cost in the short term to hire the outside agency or develop the computer based program, it would generally reduce costs in the future. Current training uses Corporate Security agents as instructors. It was determined that it is best to use Corporate Security agents as they provide greater insight into Company employees, history, locations, and operations. Accordingly, this alternative was dismissed. However, as demand increases for security related training, it may be necessary to review and/or further explore alternatives.

9.2 Alternative 2 – Physical Security Tradeoffs

Physical security systems (cameras, fences, etc.) and guards may be used as alternatives to each other depending on the facility and the threat. This would mean that some SoCalGas locations would only have security guards while others would only have security systems. The alternatives are considered for each individual facility and may be based upon threat level, vulnerably, visibility, location, costs, operations, etc. The potential benefit to this alternative is a reduction of costs; however, it would also

increase the risk exposure. Accordingly, this alternative was dismissed in favor of the proposed plan – that is, implementing physical security systems and guards because they often provide increased risk reduction and can be a back-up to one another.