Risk Assessment Mitigation Phase
Risk Mitigation Plan

Workplace Violence
(Chapter SDG&E-9/SCG-5)

November 30, 2016

TABLE OF CONTENTS

Executive Summary

The purpose of this chapter is to present the mitigation plan of the San Diego Gas & Electric Company (SDG&E) and Southern California Gas Company (SoCalGas) (collectively, the Companies) for the risk of Workplace Violence. The Workplace Violence risk involves a violent incident related to the workplace, resulting in emotional or physical harm to an employee(s) or third parties. The Companies' 2015 baseline mitigation plan for this risk consists of four controls:

1. Physical Security Systems
2. Contract Security
3. Planning, Awareness, and Incident Management
4. Training

These controls focus on safety-related impacts (i.e., Health, Safety, and Environment) per guidance provided by the California Public Utilities Commission (Commission or CPUC) in Decision 16-08-018, as well as controls and mitigations that may address reliability. The Companies' proposed mitigation plan comprises both baseline and new mitigation activities. The Companies are proposing to continue supporting their physical security systems and contract security personnel.

Based on the foregoing assessment, the Companies proposed future mitigations. Generally, the baseline projects described above have been completed and placed into service. For Workplace Violence, the Companies proposed to continue the four control categories, identified above, but included enhancements within each category. The enhancements include:

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
    - Upgrade or replace the incident/case management system
    - Add social media monitoring tool
    - Add personnel in the risk management and corporate security areas

The risk spend efficiency (RSE) is a new tool that was developed to attempt to quantify how the proposed mitigations will incrementally reduce risk. The RSEs for Workplace Violence are evaluated at the risk portfolio level, with the activities grouped into one, aggregated mitigation.

Risk: Workplace Violence

1 Purpose

The Companies consider workplace violence to be a violent incident related to the workplace, resulting in emotional or physical harm to an employee(s) or third parties. Emotional harm or distress includes, but is not limited to, mental distress, mental suffering, or mental anguish. Physical harm refers to any physical injury to the body, including an injury that caused, either temporarily or permanently, partial or total physical disability, incapacity or disfigurement.

This risk is a product of the Companies' 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. Note that while 2015 is used a base year for mitigation planning, risk management has been occurring, successfully, for many years within the Companies. The Companies take compliance and managing risks seriously, as can be seen by the numerous actions taken to mitigate each risk. This is the first time, however, that the Companies 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 Companies do not currently track expenditures in this way, so the baseline amounts are the best effort of the Companies 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 Commission 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 Companies 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 Companies have made efforts to identify those costs.
This risk assessment focuses on the drivers or factors that could potentially cause an incident and result in potential consequences. Drivers and events that are unknown to the Companies are outside the scope of this risk. Further, this chapter focuses on events that could potentially occur at the Companies' facilities. However, any actions that could result in emotional or physical harm to employees or third

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

parties related to the workplace for which the Companies are reasonably aware, regardless of the facility type, are within the scope of this risk.

2 Risk Information

As stated in the testimony of Jorge M. DaSilva in the Safety Model Assessment Proceeding (S-MAP) Applications (A.) 15-05-002/004, "SDG&E[/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."[2] The Enterprise Risk Management (ERM) process and lexicon that the Companies have put in place were built on the internationally-accepted IS0 31000 risk management standard. In the application and evolution of this process, the Companies are committed to increasing the use of quantification within its evaluation and prioritization of risks.[3] This includes identifying leading indicators of risk. Sections 2 – 8 of this plan 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 Workplace Violence risk.

2.1. Risk Classification

Consistent with the taxonomy presented by the Companies in A.15-05-002/004, the Companies classify this as a cross-cutting risk that affects people and is a function of employee or former employee conduct. Workplace Violence is a cross-cutting risk because an incident could occur in any department of the company. The risk classification is provided in

Table 1.

Table 1: Risk Classification per Taxonomy

Risk Type	Asset/Function Category	Asset/Function Type
CROSS-CUTTING	PEOPLE	EMPLOYEE CONDUCT

[2] A.15-05-002/004, filed May 1, 2015, at p. JMD-7.
[3] Testimony of Diana Day, Risk Management and Policy (SDG&E-02), submitted on November 14, 2014 in A.14-11-003.

2.2. Potential Drivers[4]

When performing the risk assessment for Workplace Violence, the Companies identified potential indicators of risk, referred to as drivers, that could potentially lead to a Workplace Violence incident. These include, but are not limited to, the following drivers as defined below:

- **Human Error** – an error that occurs due to someone not doing something correctly.
- **Process Failure** – an inadequacy in programs/procedures that are intended to help avoid the risk from occurring and control the consequence of the risk if it occurs.
- **System Failure** – an inadequacy in security systems that are intended to help avoid the risk from occurring.

In addition to the above potential drivers, the Companies have identified potential circumstances that could contribute to Workplace Violence. These include, but are not limited to: extremist ideologies, personal issues or conflict, and mental health issues.

These potential drivers and circumstances are not intended to be a comprehensive list, as the types of workplace violence incidents vary greatly. The potential drivers and circumstances noted in this plan correspond with those in studies, such as the New York City Police Department's "Active Shooter: Recommendations and Analysis for Risk Mitigation" and the Federal Bureau of Investigation's "A Study of Active Shooter Incidents in the United States Between 2000 and 2013." These studies provide analysis of active shooter incidents showing a wide range of motivations, including domestic quarrels, professional differences, and mental health issues.

2.3. Potential Consequences

If one of the drivers listed above were to occur, resulting in an incident, the potential consequences, in a reasonable worst case scenario, could include:

- Emotional abuse, injury, or fatality;
- Operational disruptions;
- Citations, adverse litigation, and related financial impacts; and/or
- Costs associated with policy/procedure changes.

These potential consequences were used in the scoring of the Workplace Violence risk that occurred during the Companies' 2015 risk registry process. See Section 3 for more detail.

2.4. Risk Bow Tie

The risk "bow tie," shown in Figure 1, is a commonly-used tool for risk analysis. The left side of the bow tie illustrates potential 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.

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

Figure 1: Risk Bow Tie

3 Risk Score

The Companies' ERM organization facilitated the 2015 risk registry process, which resulted in the inclusion of Workplace Violence as one of the enterprise risks. During the development of the risk registry, subject matter experts (SMEs) assigned a score to this risk, based on empirical data to the extent it was available and/or using their expertise, following the process outlined in this section.

3.1. Risk Scenario – Reasonable Worst Case

There are many possible ways in which a Workplace Violence risk event can occur. For purposes of scoring this risk, SMEs used a reasonable worst case scenario to assess the impact and frequency. The scenario represented a situation that could happen, within a reasonable timeframe, and lead to a relatively significant adverse outcome. These types of scenarios are sometimes referred to as low frequency, high consequence events. The SMEs selected the following reasonable worst case scenario to develop a risk score for Workplace Violence:

- An active shooter at a well-populated SDG&E facility takes action, which results in injuries and fatalities.

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

3.2. 2015 Risk Assessment

Using this scenario, SMEs then evaluated the frequency of occurrence and potential impact of the risk using the Companies' 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.[5] Using the levels defined in the REF, the SMEs applied empirical data to the extent it was 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 2 provides a summary of the Workplace Violence risk score in 2015. This risk has a score of 4 or above in the Health, Safety, and Environmental impact area and, therefore, was included 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 2: Risk Score

Residual Impact				Residual Frequency	Residual Risk Score
Health, Safety, Environmental (40%)	Operational & Reliability (20%)	Regulatory, Legal, Compliance (20%)	Financial (20%)		
6	1	2	3	3	23,107

3.3. Explanation of Health, Safety, and Environmental Impact Score

Based on the risk scenario of an active shooter at a well-populated company facility, such an incident could result in a few life-threatening injuries and/or fatalities. A Federal Bureau of Investigation's report, "A Study of Active Shooter Incidents in the United States Between 2000 and 2013," states that 160 active shooter incidents occurred, with 486 deaths and 557 injured people, over the 13-year span of the study. The report also explains that the number of individuals killed or injured during an active shooter incident has increased as well.

Notably, in December 2011, Southern California Edison Company (SCE) experienced a workplace shooting at its office complex in Irwindale by an alleged SCE employee, resulting in multiple injuries and fatalities.[6] Another shooting incident in 2009, involving two current and one former SoCalGas employees, left three people dead.[7]

Accordingly, SDG&E scored Workplace Violence a 6 (Severe) in the Health, Safety, and Environmental impact area, as there could likely be several fatalities and/or life threatening injuries based on the risk

[5] D.16-08-018 Ordering Paragraph 9.
[6] http://articles.latimes.com/2011/dec/17/local/la-me-shooting-follow-20111218.
[7] http://www.washingtontimes.com/news/2009/mar/19/suspect-in-killing-of-socal-gas-workers-found-shot/.

scenario. A 7 (Catastrophic) did not seem appropriate, as this score would reflect a large-scale event with a high number of deaths and/or irreversible impacts to the environment.

3.4. Explanation of Other Impact Scores

Based on the selected reasonable worst case risk scenario, the Companies gave the following scores to the remaining impact categories:

- **Operational and Reliability**: Workplace Violence was scored a 1 (Insignificant) as it is likely that the Companies' primary operations of gas and electricity transmission and distribution would continue, and that there would be minimal disruption to service, if a Workplace Violence incident were to occur. This rating focused on the overall operational capability of the Companies and service impact to customers; it did not rate the level of impact to an individual business unit.
- **Regulatory, Legal, and Compliance**: Workplace Violence was scored a 2 (Minor) as the potential for regulatory penalties with respect to an active shooter incident is anticipated to be minimal (if any). The potential legal issues associated with this risk are most likely to be civil in nature; the potential impacts of these legal issues are addressed in the Financial impact area.
- **Financial**: Workplace Violence was scored a 3 (Moderate) as there could be potential financial impacts to the company from potential litigation (e.g., a wrongful death lawsuit) and possible associated costs for security remediation and upgrades, training programs, and potential policy/procedures changes. Although it is difficult to predict the amount of litigation a company may face after an active shooter incident, based on the risk scenario, the Companies estimated that potential costs could be between $1 million and $10 million.

3.5. Explanation of Frequency Score

The SMEs considered an active shooter incident to occur infrequently (a score of 3), which is defined as having the potential to occur every 10-30 years in the company's service territory. As a comparison, it was assumed that facilities with a history of active shooting incidents, such as schools or government facilities, may merit a score of 4 (Occasional), which is defined as occurring every 3-10 years. There have been few active shooter incidents specific to the utility industry; however, the Companies did not consider it to be appropriate to elevate the rating higher than a 3.

4 Baseline Risk Mitigation Plan[8]

As stated above, Workplace Violence risk involves a violent incident related to the workplace, resulting in emotional or physical harm to an employee(s) or third parties. The 2015 baseline mitigations discussed below include the current evolution of the Companies' management of this risk. The baseline mitigations have been developed over many years to address this risk. They include the amount to comply with laws that were in effect at that time. The Companies' mitigation plan for this risk includes the following controls:

[8] As of 2015, which is the base year for purposes of this Report.

- Physical Security Systems and Contract Security
- Planning, Awareness, and Incident Management
    - Workplace Violence Mitigation Team
    - Training
    - Investigations
    - Employee awareness
    - New-hire screening processes
    - Employee Assistance Program(s)
    - Incident/Case Management System
    - Risk Management Program

SMEs from Corporate Security, which is a function of the Companies' parent company Sempra Energy, and each company's Human Resources (HR) department collaborated to identify and document them. These controls focus on safety-related impacts[9] (i.e., Health, Safety, and Environment) per guidance provided by the Commission in D.16-08-018,[10] as well as controls and mitigations that may address reliability.[11] Accordingly, the controls and mitigations described in Sections 4 and 5 primarily address safety-related impacts. Note that the controls and mitigations in the baseline and proposed plans are intended to address various Workplace Violence incidents, not just the scenario used for purposes of risk scoring.

The United States Department of Labor outlines the components of an effective workplace violence program,[12] including:

- Work Environment – creating a professional, healthy, and caring work environment
- Security – maintaining a secure and physically safe workplace
- Education – communicating awareness regarding workplace violence
- Performance / Conduct Indicators – identifying conduct that may present warning signs
- Employee Support Services – assisting employees in dealing with personal/professional issues

The Companies' workplace violence mitigation plans address each of these components as described below.

1. <u>Physical Security Systems and Contract Security</u>

[9] The Baseline and Proposed Risk Mitigation Plans may include mandated, compliance-driven mitigations.
[10] 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 of RAMP is to "make California safer by identifying the mitigations that can optimize safety."
[11] Reliability typically has an impact on safety. Accordingly, it is difficult to separate reliability and safety.
[12] https://www.dol.gov/oasam/hrc/policies/dol-workplace-violence-program.htm.

The purpose of physical security is to maintain the safety of employees, contractors, and the public, as well as the Companies' facilities, through the use of systems, personnel, policies, and procedures. Two physical security mitigation activities in the current risk mitigation plan align with this purpose: physical security systems and contract security (e.g., security guards).

Security enhancements to infrastructure and security guards posted at company facilities each improve access control, intrusion detection, and interdiction capabilities, to deter, detect, delay, or help prevent undesirable events at company facilities. Depending on the facility, several physical security system upgrades have been completed, including, but not limited to, improvements with access control, intrusion detection systems, and interdiction capabilities.

In addition to security systems, the Companies employ contract security (security guards) to secure and physically protect assets and people. These security guards are located at critical facilities and work locations. Company policies and procedures outline physical security procedures, including access control, officer post orders and incident reporting.

2. Planning, Awareness, and Incident Management

The Planning, Awareness, and Incident Management mitigation includes projects and programs that largely provide services to try to manage this risk before an event can occur. These mitigations consist of the Workplace Violence Mitigation Team, training, investigations, employee awareness, new hire screening processes, employee assistance and wellness programs, and Corporate Security's risk management program. Each is discussed below.

Workplace Violence Mitigation Team (WVMT)

The Workplace Violence Mitigation Team (WVMT), formed in 2011, is a joint team of Managers, Directors, or Vice President level representatives within Corporate Security, HR, and Legal. The team is specifically trained to assess and respond to the threat posed by an individual that may be prone to violence. The WVMT is responsible for developing and executing an effective Workplace Violence Prevention program that includes, but is not limited to:

- Training supervisors and employees to detect early warning signs of possible workplace violence;
- Investigating and mitigating potential workplace violence incidents;
- Responding appropriately to threat-related emergencies;
- Identifying and enlisting the assistance of qualified professionals in workplace violence assessment, security, and incident management; and
- Documenting all activities related to workplace violence prevention and control.

The WVMT uses various threat management tools provided by outside professional resources or developed and adapted by the WVMT. These tools are intended to guide the WVMT in their data

collection and decision making throughout the management of a case. The tools may be used in conjunction with appropriate degrees of professional threat management consultation.

The WVMT meets as needed when an individual displays signs that he/she may be prone to violence or engage in violent action on company property. Upon notification of an alleged threat, an initial investigation helps determine if additional action is warranted.

A recent third-party review of Sempra Energy security and investigative programs stated: "The Sempra approach to Workplace Violence Mitigation Teams is considered to be of a high caliber. We have identified this as an area where Sempra has adopted 'leading practices' in the area of workplace violence prevention."

Training

The Companies offer a variety of training opportunities to employees to increase awareness regarding the identification and response to criminal activity, including workplace violence. Examples include, but are not limited to: Active Shooter Training, Security Awareness Training, Workplace Violence Training, and Hostile Intruder Training. A few are described in more detail below.

Active Shooter Training has been provided to thousands of employees and focuses on the actions employees should take during an active shooter scenario. The training was developed by Corporate Security, and is based upon the Department of Homeland Security (DHS) training titled “Run, Hide, Fight.” Through interactive discussion, this training provides basic awareness of recognizing an active shooter situation and how to respond accordingly. Topics include:

- Active Shooter Definition
- Active Shooter Incidents
- Active Shooter Characteristics and Triggers
- Run, Hide, Fight
- Last Resort Survival Measures
- Police Arrival
- Preparation

This training goes beyond a simple explanation of the issue, and provides employees with actions to take during an active shooter incident, including considerations for evacuation, appropriate hiding locations and instructions, and, when necessary, how to take action when confronted with an active shooter. The training also offers reporting procedures and proper conduct when police arrive.

Corporate Security also provides *Security Awareness Training* to employees, which focuses on identifying threats and suspicious activity, response to threats, and proper reporting protocols. *Workplace Violence training* is provided every other year by two board-certified forensic psychologists who consult to numerous federal, state, and local law enforcement agencies. This training instructs on

the use of Workplace Assessment of Violence Risk (WAVR-21), a screening tool used by workplace violence mitigation teams.[13]

As discussed in the following section, Corporate Security recommends this training continue to be offered through regular instructor-led sessions or through online viewing of materials provided on the Corporate Security website.

Investigations

Corporate Security agents investigate hundreds of incident reports each year, including, but not limited to, disruptive incidents, burglary, theft, employee misconduct, and suspicious activity. Corporate Security works closely with Legal, HR, affected business units, and, when necessary, law enforcement, to thoroughly investigate allegations of workplace violence. This process assists with gathering or validating information needed for decision makers to act accordingly.

Employee Awareness

The Companies use a variety of methods to increase employee awareness, including, but not limited to: emergency and incident planning, training, education, drills, and communication. Workplace violence, safety, and security awareness training is provided on a regular basis to employees. Evacuation plans have been developed, updated, trained, and drilled. Security alerts and bulletins are provided as needed through email and posted on digital message boards, or on the company website. In addition, an emergency notification system, often referred to as a reverse 911 system, is in place to rapidly distribute emergency information to employees. This system will call, text, and email employees so that emergency messages are distributed efficiently and effectively. These efforts can provide employees with a heightened security awareness and effective communication platforms to assist with mitigation of security incidents, including workplace violence.

New Hire Screening Processes

There may be several reasons for performing new hire screening for job applicants. Some job duties are conducted in potentially hazardous environments. In these circumstances, the Companies take steps to try to avoid hiring that could result in safety or security incidents. The importance of the electric and natural gas transmission and distribution systems, including their interdependency with life/safety, emergency response, and national security, also provides a basis for heightened security and identity-verification processes. The Companies perform new hire screening in accordance with federal, state, and local laws.

[13] http://www.wavr21.com/

Employee Assistance and Wellness Programs

Some workplace violence incidents are a result of domestic, financial, health, substance abuse, or other types of issues, which may have the potential to be resolved with employee assistance programs. As described on the company website, since their inception in 1990, the Energy For Life Wellness Programs have been committed to enhancing the physical and mental well-being of all company employees through programs, resources, information, and support services that promote safe and healthy lifestyles.

These company-provided wellness programs are offered to all employees through methods such as on-site and online services, work groups, health fairs, fitness programs, and educational brochures. In addition, the Employee Assistance Program (EAP) is a confidential counseling and referral service to help employees' family members deal with life's daily challenges. These services may assist employees with personal and/or work-related problems that may impact their job performance, health, mental, and emotional well-being. As stated above, the Department of Labor outlines the importance of early intervention in the prevention of workplace violence, including employee assistance and wellness programs.

Employees have access to the 24/7 support services if they feel threatened by another employee. Every matter reported will be investigated by the company and, if requested, a response given to the individual reporting the issue. If necessary, the matter may be referred to staff or outside counsel for professional evaluation and recommendations on how to respond. This mitigation is recognized by the Department of Labor as a critical component in the prevention of workplace violence and should continue to be provided and updated as necessary.

Incident/Case Management System

Corporate Security maintains an incident/case management system to track incidents and investigations, such as, burglary, theft, vandalism, and workplace violence. The system provides data necessary for analysis of security programs, and assists with strategic planning to improve security and safety of company facilities, employees, and the public.

Risk Management Program

Corporate Security has established an intelligence program to collect, analyze, and disseminate intelligence that may assist with decision making regarding energy operations and security procedures. An intelligence program helps anticipate, identify, and assess threats that could harm the company, its employees, guests, or assets, and provides actionable strategic and tactical intelligence to mitigate risk. The program develops and maintains regular contact with local, national, and international law enforcement and intelligence community partners on a regular basis. The program also creates a risk management process to prioritize and mitigate threats, vulnerabilities, and consequences. Threat assessments and security plans specific to company infrastructure support regulatory requirements.

5 Proposed Risk Mitigation Plan

The 2015 baseline mitigations outlined in Section 4 will continue to be performed in the proposed plan, in most cases, to maintain the current residual risk level. In addition, the Companies are proposing during the 2017-2019 timeframe to expand or add the mitigations addressed below.

1. Physical Security Systems and Contract Security

The Companies are proposing to continue supporting their physical security systems and contract security personnel. The purpose of these activities is to reduce the likelihood of a Workplace Violence event by increasing protective measures at company facilities that have employees.

Generally, the baseline projects described above have been completed and placed into service. The Companies are proposing to complete similar security projects to increase protection, such as installing or updating access control and detection capabilities at facilities that have employees. Similarly, the presence of security guards increases protection with the aim of reducing the likelihood of an intentional event.

There are two expanded activities, as compared to the baseline, with respect to security guards. First, the Companies propose to add security guards to new locations. Second, SDG&E must comply with Senate Bill (SB) 3, which will become effective January 1, 2017. The resulting effects are increases in costs above the GRC standard escalation. In other words, the cost associated with doing business (i.e., employing security guards) has increased. This is sometimes referred to as non-standard escalation.

2. Planning, Awareness, and Incident Management

This mitigation consists of expanded and new activities: upgrade or replacement of the incident/case management system; addition of social media monitoring tool; and additional personnel in the risk management and corporate security areas.

Incident/Case Management System

The current incident/case management system manages security incidents by capturing information from investigations and providing historical querying capability. This system is approximately ten years old. With the increase of requests for information and data calls from state and federal regulatory entities, it is recommended that this system be upgraded or replaced. The current system does not allow for querying of data at the appropriate level of detail. Simple changes that may provide some additional functionality to assist with querying will be expensive and may only provide some of the necessary upgrades. It is possible alternate systems already used by Sempra may provide suitable incident/case management services to meet this increased need. Costs of upgrading the existing system are currently being compared to other options.

Social Media Monitoring

Many utilities, other private sector companies, and public agencies are using social media monitoring for emergency notifications, incident updates, threat identification, customer communications, and to identify the misuse of branding. In a security setting, these tools can provide real-time updates to incidents, which may affect the safety or security of employees. These tools also can provide insight into emerging or imminent threats to company employees or infrastructure.

Risk Management

Based on new federal and state laws, the Companies are required to provide additional workplace violence risk management. The Companies are required to identify and prioritize threats, vulnerabilities, and consequences due to federal and state mandates and requests for information. In addition, this information will assist with security planning and mitigation development. Currently, Corporate Security has one risk/intelligence analyst. Given the increase in workload due to increased regulations, another resource is needed.

Corporate Security Agent

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. Currently, SDG&E's Corporate Security has two agents covering the security for the entire service area, 4,300 employees, 3.6 million customers, and all facilities. SoCalGas' Corporate Security has four agents covering the security for the entire service area, 8,400 employees, 21 million customers, and approximately 130 facilities.

6 Summary of Mitigations

Tables 3a and 3b summarize the 2015 baseline risk mitigation plan, the risk driver(s) a control addresses, and the 2015 baseline costs for Workplace Violence. 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.

The Companies do 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.

While all the controls shown on Table 3a and 4b mitigate Workplace Violence, some of the controls also mitigate other risks presented in this RAMP Report. Specifically, for SDG&E, Physical Security Systems and Contract Security, managed by Corporate Security, also help mitigate the RAMP risk of Public Safety Events - Electric. Accordingly, because the benefits associated with these activities can be attributed to both this risk and Public Safety Events - Electric, the costs are presented in both chapters.

For SoCalGas, 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 Physical Security of Critical Infrastructure. Accordingly, because there are benefits associated with these activities attributed to both this risk and Physical Security of Critical Infrastructure, the costs are also presented in both chapters.

Table 3a: SDG&E Baseline Risk Mitigation Plan[14]
(Direct 2015 $000)[15]

ID	Control	Risk Drivers Addressed	Capital[16]	O&M	Control Total[17]	GRC Total[18]
1	Physical Security Systems Contract Security	• Human Error • Process Failure • System Failure	 $3,450 840	 $400 3,930	 $3,850 4,770	 $3,850 4,770
2	Planning, Awareness, and Incident Management	• Human Error • Process Failure • System Failure	250	290	540	540
	TOTAL COST		$4,540	$4,620	$9,160	$9,160

***** Includes one or more mandated activities

[14] Recorded costs were rounded to the nearest $10,000.
[15] The figures provided in Tables 3a, 3b, 4a and 4b are direct charges and do not include company loaders, with the exception of vacation and sick. The costs are also in 2015 dollars and have not been escalated to 2016 amounts.
[16] Pursuant to D.14-12-025 and D.16-08-018, the Companies provided 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.
[17] 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).
[18] The GRC Total column shows costs typically presented in a GRC.

Table 3b: SoCalGas Baseline Risk Mitigation Plan[19]
(Direct 2015 $000)

ID	Control	Risk Drivers Addressed	Capital[20]	O&M	Control Total[21]	GRC Total[22]
1	Physical Security Systems Contract Security	• Human Error • Process Failure • System Failure	$90 40	$210 1,670	$300 1,710	$300 1,710
2	Planning, Awareness, and Incident Management	• Human Error • Process Failure • System Failure	10	420	430	430
	TOTAL COST		$140	$2,300	$2,440	$2,440

***** Includes one or more mandated activities

Tables 4a and 4b summarize the Companies' proposed mitigation plan (which comprises both baseline and new mitigation activities) and 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 the Companies are identifying potential ranges of costs in this plan, and are not requesting funding approval. The Companies will request approval of funding in their next GRC. There are non-CPUC jurisdictional mitigation activities addressed in RAMP; the costs associated with these will not be carried over to the GRC. As set forth in Tables 4a and 4b, the Companies are using a 2019 forecast provided in ranges based on 2015 dollars.

[19] Recorded costs were rounded to the nearest $10,000.
[20] Pursuant to D.14-12-025 and D.16-08-018, the Companies provided 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.
[21] 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).
[22] The GRC Total column shows costs typically presented in a GRC.

Table 4a: SDG&E Proposed Risk Mitigation Plan[23]
(Direct 2015 $000)

ID	Mitigation	Risk Drivers Addressed	2017-2019 Capital[24]	2019 O&M	Mitigation Total[25]	GRC Total[26]
1	Physical Security Systems Contract Security	• Human Error • Process Failure • System Failure	$12,040 - 14,720 2,660 - 2,950	$370 - 400 6,400 - 7,170	$12,410 - 15,120 9,060 - 10,120	$12,410 - 15,120 9,060 - 10,120
2	Planning, Awareness, and Incident Management	• Human Error • Process Failure • System Failure	530 - 580	530 - 720	1,060 - 1,300	1,060 - 1,300
	TOTAL COST		$15,230 - 18,250	$7,300 - 8,290	$22,530 - 26,540	$22,530 - 26,540

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

[23] Ranges of costs were rounded to the nearest $10,000.
[24] 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 the Companies' Test Year 2019 GRC Applications.
[25] The Mitigation Total column includes GRC items as well as any applicable non-GRC items.
[26] The GRC Total column shows costs typically represented in a GRC.

Table 4b: SoCalGas Proposed Risk Mitigation Plan[27]
(Direct 2015 $000)

ID	Mitigation	Risk Drivers Addressed	2017-2019 Capital[28]	2019 O&M	Mitigation Total[29]	GRC Total[30]
1	Physical Security Systems Contract Security	• Human Error • Process Failure • System Failure	$1,660 - 2,420 410 - 460	$150 - 230 3,450 - 3,700	$1,810 - 2,650 3,860 - 4,160	$1,810 - 2,650 3,860 - 4,160
2	Planning, Awareness, and Incident Management	• Human Error • Process Failure • System Failure	30 - 33	670 - 890	700 - 920	700 - 920
	TOTAL COST		$2,100 - 2,910	$4,270 - 4,820	$6,370 - 7,730	$6,370 - 7,730

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

1. Physical Security and Contract Security

The capital cost estimates for physical security systems were zero-based, derived from projections used to seek internal approval. The O&M costs were estimated as a percentage of the capital costs using subject matter expertise and experience with historical projects.

The physical security systems are largely capital projects. While the projects will change (e.g., expansion to additional locations), the projected annual spend is anticipated to be in line with historical spending. This estimate is only for physical security systems of manned locations that

[27] Ranges of costs were rounded to the nearest $10,000.
[28] 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 the Companies' Test Year 2019 GRC Applications.
[29] The Mitigation Total column includes GRC items as well as any applicable non-GRC items.
[30] The GRC Total column shows costs typically represented in a GRC.

may have a risk of Workplace Violence. Unmanned locations, such as substations, were not included in this calculation.

The costs for security guards are based on a five-year average labor cost, plus the cost of complying with SB 3, plus the cost of additional guarded locations. The five-year average was used as there was no discernable trend from 2011-2015.

2. Planning, Awareness and Incident Management Mitigation
The cost estimates for many of the activities (e.g., training, awareness, screening, employee assistance) in this group were based on applicable, historical costs. For some activities that were anticipated to increase, the Companies used the 2015 base year amounts and added the costs related to incremental activities. The range provides flexibility as the Companies finalize the scope of the mitigation activities.

   For the proposed incident/case management system mitigation, costs of upgrading the existing system are currently being compared to other options available on the market. The range for this activity in the proposed plan took into account the variability of pricing when upgrading this system.

   Corporate Security has received several presentations, demonstrations, and trial periods of social media monitoring tools ranging from $25,000 to $100,000. Some of the more beneficial tools may cost around $65,000 per year. Accordingly, the range for this activity reflects the price variations of such tools.

   Additional personnel are included in the proposed plan: one for Corporate Security's risk management function and one Corporate Security agent. A range was provided based on an average salary as the actual costs will depend upon the individuals' experience.

7 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."[31] 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.[32]

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

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 6). The Company applied this calculation to each of the mitigations or mitigation groupings, then ranked the proposed mitigations in accordance with the RSE result.

7.1. 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.

7.1.1 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 2 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.[33] For incremental mitigations, the analysis assesses the anti–cipated reduction of the risk if the new mitigations are implemented. The change in risk score is the risk reduction attributable to each mitigation.

7.1.2 Calculating Risk Spend Efficiency

The Company SMEs then incorporated the mitigation costs from Section 6. They multiplied the risk reduction developed in subsection 0 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 Tables 4a and 4b 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.

7.2. Risk Spend Efficiency Applied to This Risk

SDG&E and SoCalGas analysts used the general approach discussed in Section 7.1, above, in order to assess the RSE for the Workplace Violence risk. The RAMP Approach chapter in this Report provides a more detailed example of the calculation used by the Company.

This analysis used a metric (or proxy) – the national victimization rate for all crimes – to assess risk reduction. The Federal Bureau of Justice Statistics (BJS), within the Department of Justice, compiles victimization information through annual, comprehensive surveys. There are crimes with human victims and victimless crimes. The Federal surveys are meant to capture information on the former type. Survey information represents national statistics and does not contain data that can be used to separate workplace events from other events.

The Utilities compile crime information of both types as well. The categories of crime information collected by the Federal government and the Company are:

- Federal: robbery, rape/sexual assault, simple assault, and aggravated assault.
- Corporate: robbery, indecent exposure, workplace violence, and assault.

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

There is not an exact match between the crime information collected by both entities, but the data collected is similar enough to make reasonable comparisons.

An assumption of this analysis is that a victimization rate comparison reflects how safe or how unsafe a workplace environment is, and that this difference in crime exposure can be used as a proxy to evaluate the risk scenario. This proxy seems reasonable because it enables the comparison of the Utilities' workplace experience over time to the national experience; representing "at work" and "not at work" possibilities. It should be noted the Utilities' victimization rates include all threatening communication, not physical assaults only, as the BJS uses. Where applicable, the more conservative estimate was used for calculation.

The risk reduction for current controls (analyzed as one group) was calculated by determining the percent decrease from the highest victimization rate between 2010-2014 (either internal Company data or BJS data) to the 2014 internal Company victimization rate. The risk reductions from incremental mitigations (analyzed as one group) were determined by estimating the percent decrease of the residual risk (2014 internal Company rate) resulting from these proposed activities. Subject matter experts estimated this decrease to be 10%. For comparison purposes, victimization rates were calculated "per thousand people," with BJS rates representing the U.S. population and internal Company rates representing the number of respective Company employees.

SDG&E's highest victimization rate over this period occurred in 2010 and was 31.2 victimizations per thousand people (employees) per year. The national average over this period is 18.6 victimizations per thousand people per year. The higher of these two figures is used for improvement calculations and results in a baseline victimization rate decrease of 22.4 or 72%. The incremental mitigations are estimated to provide a 10% decrease of the residual risk (SDG&E 2014 victimization rate).

SoCalGas' highest victimization rate over this period occurred in 2012 and was 53.8 victimizations per thousand people (employees) per year. The national average over this period is 18.6 victimizations per thousand people per year. The higher of these two figures is used for improvement calculations and results in a baseline victimization rate decrease of 12.1 or 23%. The incremental mitigations are estimated to provide 10% decrease of the residual risk (SoCalGas 2014 victimization rate).

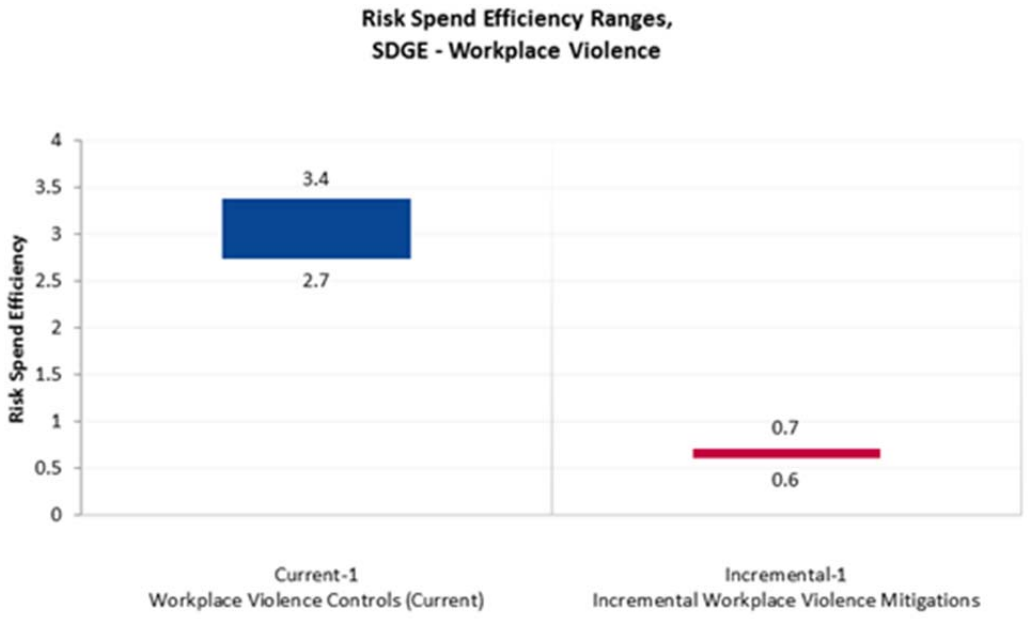
7.3. Risk Spend Efficiency Results

Based on the foregoing analysis, the utilities 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. Workplace Violence Controls
2. Incremental Workplace Violence Mitigations

Figures 3 and 4 display the range[34] of RSEs for each of the utilities' Workplace Violence risk mitigation groupings, arrayed in descending order.[35] That is, the more efficient mitigations, in terms of risk reduction per spend, are on the left side of the chart.

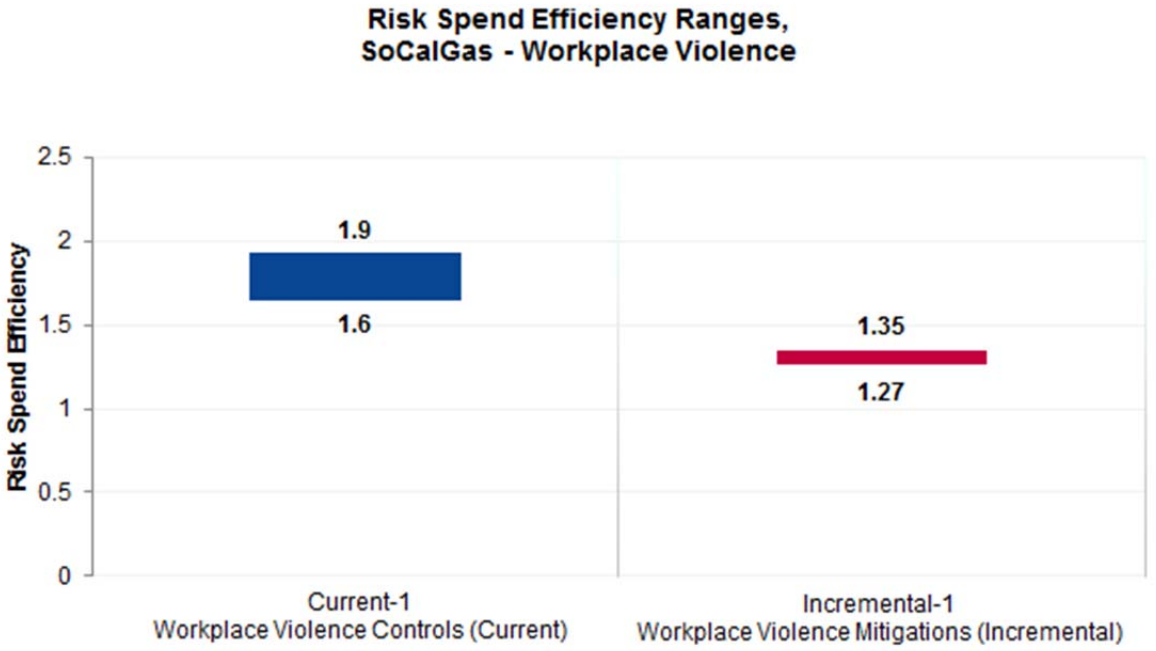
Figure 3: SDG&E Risk Spend Efficiency



[34] Based on the low and high cost ranges provided in Tables 4a and 4b of this chapter.

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

Figure 4: SoCalGas Risk Spend Efficiency



8 Alternatives Analysis

The Companies considered alternatives to the proposed mitigations as it developed the incremental mitigation plan for the Workplace Violence risk. Typically, alternatives analysis occurs when implementing activities, and with vendor selection in particular, to obtain the best result or product for the cost. The alternatives analysis for this risk plan also took into account modifications to the proposed plan and constraints, such as budget and resources. The following represents alternatives for training and for physical security. The viability of each alternative was determined through discussions with stakeholders.

8.1. Alternative 1 – Training Changes

A potential alternative for training is to outsource training or develop computer-based training. Although this alternative may have an increased cost in the short term (i.e., to hire the outside agency or develop the training), it would generally reduce costs in the future. Current training uses Corporate Security agents as instructors. Ideally, 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 further explore alternatives.

8.2. Alternative 2 – Physical Security Tradeoffs

Physical security systems (cameras, fences, etc.) and guards may be used as alternatives to each other in some locations for some threats. This would mean that some company locations would only have security guards while others would only have security systems. 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. Implementing physical security systems and guards together often provides increased risk reduction and provides a back-up to one another.