Risk Assessment Mitigation Phase
Risk Mitigation Plan
Cyber Security
(Chapter SDG&E-7/SCG-3)

November 30, 2016

310314

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 Cyber Security. The Cyber Security risk involves a major cyber security incident that causes disruptions to electric or gas operations (e.g., SCADA system) or results in damage or disruption to company operations, reputation, or disclosure of sensitive data. The Companies' 2015 baseline mitigation plan for this risk consists of five controls aligned with the control functions in the National Institute of Standards and Technology (NIST) Cyber Security Framework:

1. Identify;
2. Protect;
3. Detect;
4. Respond; and
5. Recover.

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 (D.) 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.

Based on the foregoing assessment, the Companies proposed future mitigations. For Cyber Security, the Companies proposed to continue the five control categories, identified above, but included enhancements within each category. The enhancements include:

1. <u>Identify</u>
   - Compliance Records Management – implement a system of recordkeeping dedicated to compliance records to better support regulatory auditing.
   - Enterprise Threat Intelligence – automate distribution of threat intelligence to business and system owners to improve Cyber Security risk awareness and engagement.

2. <u>Protect</u>
   - Web Applications and Database Firewalls – improve protective capabilities for web applications and databases to reduce the likelihood and impact of an incident.
   - Host-Based Protection – improve host-based protections for direct attacks and to prevent attackers from pivoting to a host from a neighboring host.

3. <u>Detect</u>

   - Insider Threat Detection/Prevention – leverage emerging technologies to improve the detection of insider threat activities and the related risk impacts.

- Perimeter Tap Infrastructure Redesign – improve the performance and visibility into network traffic to limit impacts of incidents.

4. Respond
   - Incident Response Secure Collaboration – implement a secure, out-of-band communication capability to coordinate and support incident response activity.
   - Security Orchestration – automate and support enhancements to the workflow related to responding to and analyzing escalated events to better manage and learn from cyber events.

5. Recover
   - Information Security technology backup and recovery – refresh backup and recovery for sensitive information security systems so as to return to a safe and secure risk posture.

The risk spend efficiency (RSE) was developed for Cyber Security. The risk spend efficiency is a new tool that was developed to attempt to quantify how the proposed mitigations will incrementally reduce risk. The set of corporate measures that are in place is assumed to reduce the likelihood of experiencing such an event from what the likelihood would be otherwise. The risk reduction calculation is based on internal self-assessment results, and these results are further based on the judgment of subject matter experts (SMEs).

The benefits assessment for this risk was completed at a risk portfolio level, where the migration activities (within the five functional control areas) were combined and assessed as one aggregated mitigation. Because cyber threats are in a constant evolutionary state, corporate countermeasures also evolve over time and are generally lagging. Since countermeasures are designed to match known threats, all of them are categorized as baseline, so only one set of security measures was analyzed.

The benefits assessment addresses the mitigations at both Companies, collectively.

Risk: Cyber Security

1 Purpose

The purpose of this chapter (or plan) is to present the combined mitigation plans of the Companies for the risk of Cyber Security. This risk is a major cyber security incident that causes disruptions to electric or gas operations (e.g., SCADA system) or results in damage or disruption to company operations, reputation, or disclosure of sensitive data.

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 number of 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 company to benchmark both capital and operations and management (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 the Risk Assessment Mitigation Phase (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.

Electric and gas operations, safety systems, information processing, and other utility functions are increasingly reliant on technology, automation and integration with other systems. The complex interoperation of these systems and the rapid changes that occur in the industry in response to climate,

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

cost and other drivers create a risk situation where inadvertent actions or maliciously motivated events can potentially disrupt core operations or disclose sensitive data, among other serious consequences. In addition, the functioning of society relies on safe and reliable energy delivery. The magnitude and likelihood of the Cyber Security risk is a documented concern at the national level, exemplified by Executive Order 13636 of February 21, 2013, titled "Improving Critical Infrastructure Cybersecurity."

This risk assessment focuses on responding to, and mitigating potential drivers and the potential resulting events of which the company is aware. However, the Companies strive to implement mitigations to address those instances (drivers and/or events) that may be unknown to the company. The mitigation approach is to leverage a framework of cyber security controls across the enterprise, with emphasis on key systems and data in order to address evolving threats and vulnerabilities. This approach considers all systems as potential weak points, which may provide an attacker a foothold within the enterprise or, through an error, create a situation to disrupt energy delivery, expose sensitive information, or cause other potential adverse events.

The assessment does not address Cyber Security risk mitigations performed by other groups within the business and Information Technology organizations. In particular, recovering and restoring energy delivery is addressed by other risks areas and departments.

The internal organization responsible for managing this risk is primarily the Information Security (IS) department, which resides in the Information Technology organization. The mitigations discussed in this chapter focus on those activities performed or supported directly by the department as a shared service for SDG&E, SoCalGas, and Sempra Energy, the parent company of SDG&E and SoCalGas. The Information Security department addresses cyber security risks potentially impacting the energy distribution information technology infrastructure and customer and business information systems.

As mentioned above, Cyber Security is a shared service since it supports SDG&E, SoCalGas and Sempra Energy. Generally, for accounting purposes, enterprise capital-funded solutions are booked to SoCalGas, while the bulk of the staffing resources and non-labor O&M costs are booked in SDG&E. Activities specific to electric appear in the SDG&E mitigation plan and activities attributed to the gas systems are addressed in SoCalGas' mitigation plan.

2 Background

In general, the Companies' Information Security Cyber Security program addresses Cyber Security at the enterprise level, using the industry standard NIST Cyber Security Framework[2] as a guide for best security risk management practices. Cyber security programs addressing this risk are not mandated; however, a cyber security program based on best practices, like the NIST framework, also should be in compliance with any forthcoming mandates. Should requirements or mandates change, the best practices followed by the program would be reviewed and updated to assess compliance.

In response to Executive Order 13636, the NIST Cyber Security Framework was developed through collaboration between the Federal government and the private sector, to address and manage Cyber Security risk cost-effectively based on business needs. The Framework supports the application of Cyber Security risk controls and best practices to reduce and manage Cyber Security risks, in order to improve the security and resilience of critical infrastructure. Effective industry practices from multiple resources have been grouped into five functional areas: (1) Identity; (2) Protect; (3) Detect; (4) Respond; and (5) Recover.

The Cyber Security risk mitigation plan is based on these functional areas. The definitions and descriptions of the functional areas are from the NIST Cyber Security Framework 1.0, pages 8-9.

1. Identify

Identify refers to developing organizational understanding to manage Cyber Security risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the NIST Framework. Understanding the business context, the resources that support critical functions, and the related cyber security risks, enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of control Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

2. Protect

Protect refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

[2] https://www.nist.gov/cyberframework.

3. Detect

Detect refers to developing and implementing the appropriate activities to identify the occurrence of a Cyber Security event. The Detect Function enables timely discovery of Cyber Security events. Examples of control Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

4. Respond

Respond refers to developing and implementing the appropriate activities to take action regarding a detected Cyber Security event. The Respond Function supports the ability to contain the impact of a potential Cyber Security event. Examples of control Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

5. Recover

Recover refers to developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recover Function supports timely recovery to normal operations to reduce the impact from a Cyber Security event. Examples of control Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.1 Safety Model Assessment Proceeding

SDG&E presented how it manages Cyber Security risk in the Safety Model Assessment Proceeding (S-MAP). On May 1, 2015, SDG&E submitted its Application (A.) 15-05-002, which was accompanied by the supporting testimony of Scott King. Mr. King described the Information Security Program and the Cyber Security risk management process. The Information Security Program governs risk management activities via the application of best practices, acceptable use policies, security standards, and technology requirements for managing and maintaining technology systems.

The Cyber Security risk management process describes the methodology used to prioritize resources to address identified risks. Risks are identified using multiple sources of information and assessments of both practices and critical cyber security controls. The risk mitigation practices and controls described in the S-MAP testimony are mapped to the NIST Cyber Security Framework to provide a programmatic summary. Efforts to manage risk are prioritized based on the risk scoring, benefits of the control activity, and evolving threats to the safety and reliability of critical systems.

Managing Cyber Security risk is a key business practice at the Companies that continually evolves to keep pace with threats, technology innovations, and advances in cyber security best practices to efficiently and cost-effectively manage cyber-related risks. The NIST cyber security framework is used to group these activities and projects into the five functional areas described above.

3 Risk Information

As stated in the testimony of Jorge M. DaSilva in 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."[3] The Enterprise Risk Management (ERM) process and lexicon that the Companies have put in place was 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.[4] This includes identifying leading indicators of risk. Sections 3 – 9 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 Cyber Security risk.

3.1 Risk Classification

Consistent with the taxonomy presented by SDG&E and SoCalGas in A.15-05-002, the Companies classify this risk as a cross-cutting risk that affects business and Information Technology (IT) systems as shown in 1. Cyber Security is a cross-cutting risk because an incident could potentially impact many areas throughout the Companies.

Table 1: Risk Classification per Taxonomy

Risk Type	Asset/Function Category	Asset/Function Type
CROSS-CUTTING	BUSINESS/IT SYSTEMS	TECHNOLOGY ASSETS AND INFORMATION

The threats related to this risk are dynamic. New adversarial techniques may evade current Cyber Security controls. Technology innovations and adoption continually increase the exposure of infrastructure and business services to a risk impact.

3.2 Potential Drivers[5]

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

- **Technology Failure** – The malfunction or failure of a technological device.

[3] A.15-05-002/004, filed May 1, 2015, at p. JMD-7.
[4] Testimony of Diana Day, Risk Management and Policy (SDG&E-02), submitted on November 14, 2014 in A.14-11-003.
[5] An indication that a risk could occur. It does not reflect actual or threatened conditions.

- **Human Threats** – These can be unintentional or deliberate. An unintentional threat is an error that occurs due to someone not doing something correctly. A deliberate threat includes potentially criminal activity that is likely motivated by profit, political agenda, or other illegal activity. Deliberate human threats are the most challenging threat to mitigate because tactics, methods, and capabilities evolve quickly to leverage unknown or unanticipated weaknesses.
- **Public Incident** – An incident, such as a long-term power outage, pollution, or chemical spill, motivating a threat agent to attempt to affect the risk.
- **Force of Nature** – An environmental event such as a flood, earthquake, or fire, that can cause a combination of asset, human, or process failures to circumvent controls designed to prevent the risk from occurring.

Human threat sources can be further grouped based on motivations and associated drivers. Human threat sources, motivations, and actions are described in Table from NIST SP 800-30.

Table 2: NIST SP 800-30 Threat Descriptions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

The threats identified above are an expansion of human deliberate actions that may result in the realization of a cyber event. Worldwide access to the Internet and the pervasiveness of technology leveraging networking capabilities potentially expose information and operational technology and information assets to all human threat agents. The Companies monitor such potential threats and implement mitigation efforts, as described in Sections 5 and 6, to protect the employees, contractors, customers, the public, and the Companies.

3.3 Potential Consequences

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

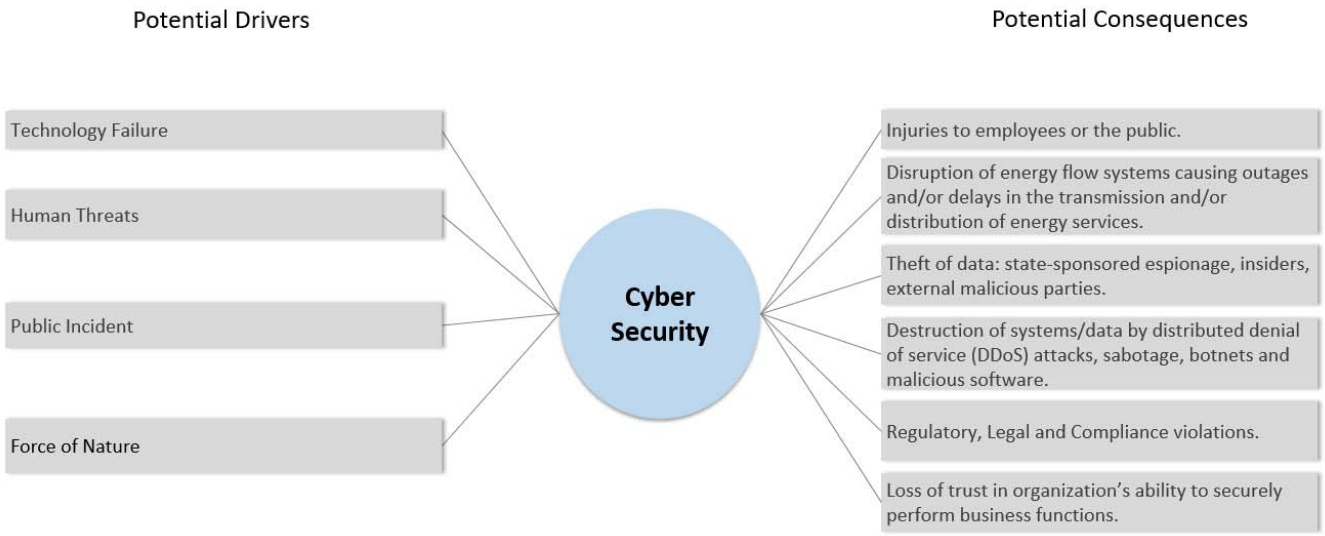
- Injuries to employees or the public.
    - Incorrect system information may result in unsafe operating conditions related to what the system operators believe to be happening versus the actual system state.
    - Loss of operational control of energy systems.
- Disruption of energy flow systems causing outages and/or delays in the transmission and/or distribution of energy services.
    - Direct impact to customer's lighting, heating, refrigeration, and other energy-related activities.
    - Social disruptions such as food distribution constraints, traffic light functions, gas distribution, water systems, telecommunications, and reliable support of other dependent industries.
- Theft of data: State-sponsored espionage, insiders, and external malicious parties.
    - Data may include system information, strategy and planning data, or other restricted or confidential information resulting in increased risk to assets, increased costs, and other business impacts.
    - Stolen customer information could be used to steal identities, perpetrate fraud or other criminal activities, or gain access to proprietary customer data.
    - Stolen data may also be used to plan and conduct exploitation of Cyber Security weaknesses or other risks.
- Destruction of systems/data by distributed denial of service (DDoS) attacks, sabotage, botnets, and malicious software.
    - The resulting impacts may include an inability to control energy delivery and other systems, failure of protective systems, loss of utility assets, customer disruption, or other system and financial impacts.
- Regulatory, Legal, and Compliance violations.
    - Breach of regulatory compliance (for example, an incident of non-compliance with NERC CIP (FERC) or a customer privacy breach (California Statutory)) resulting in adverse publicity, sanctions, and increased scrutiny of operations by the regulator.
- Loss of trust in organization's ability to securely perform business functions.
    - Business level impacts may include the inability to guard against Cyber Security incidents, technologically interact with partners, and retain employees.
    - Customer level impacts may make it difficult to collect necessary customer information and conduct other interactions, tainted by an unwillingness to share information.

These potential consequences were used in the scoring of Cyber Security that occurred during the Companies' 2015 risk registry process. See Section 4 for more detail.

3.4 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.

Figure 1: Risk Bow Tie



4 Risk Score

The Companies' ERM organization facilitated the 2015 risk registry process, which resulted in the inclusion of Cyber Security as one of the enterprise risks. During the development of the risk register, SMEs assigned a score to this risk, based on empirical data to the extent it is available and/or using their expertise, following the process outlined in this section.

4.1 Risk Scenario – Reasonable Worst Case

There are many possible ways in which a public safety 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 Cyber Security:

- An advanced, persistent threat infiltrates energy delivery management, monitoring, and safety systems to prepare for a coordinated attack that disrupts operator control systems; disables or destroys backup and redundant system protection and recovery assets; disrupts communication capabilities; and remotely launches attacks during a major local event.

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

4.2 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.[6] 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 3 provides a summary of the Cyber Security 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 3: Risk Score

Residual Impact				Residual Frequency	Residual Risk Score
Health, Safety, Environmental (40%)	Operational & Reliability (20%)	Regulatory, Legal, Compliance (20%)	Financial (20%)		
4	6	5	5	4	44,548

4.3 Explanation of Health, Safety, and Environmental Impact Score

The Companies score Cyber Security a 4 (Major) in the Health, Safety, and Environmental impact area based on the potential to cause few serious injuries to the public or employees. This is because a cyber security incident within the control systems responsible for delivering energy into the service area could disrupt energy flow systems, causing widespread outages or infrastructure malfunctions, resulting in the potential for injuries. Also, an incident could impact local areas, resulting in neighborhoods or individuals experiencing impacts to health or safety-related equipment during periods of environmental stress (heat or cold), or to the use of necessary medical equipment.

[6] D.16-08-018, Ordering Paragraph 9.

4.4 Explanation of Other Impact Scores

Based on the selected reasonable worst case risk scenario, the Companies scored each of the other residual impact areas. The scenario, for example, such as the 2015 cyber security attack on the Ukrainian Power Grid (UPG), could have an impact on more than one of the risk areas. During that remote cyber security attack, power system components were maliciously operated and automation systems were disabled, resulting in disruption of power delivery to its customers. A third party gained illegal entry into UPG computers and SCADA systems. Multiple substations were remotely controlled and disconnected. Response and recovery activities were also hindered by changes in support systems, disabled devices, and attacks on the communications systems. The incident affected up to 225,000 customers in three different service territories for several hours. Service was recovered by operating in a manual mode.[7]

There are many, frequent stories in the media about information disclosure, vulnerabilities, threat agents, and compromises. Most of these stories, when applied to the Companies, would have a similar impact in one or more of the risk areas.[8]

The other risk impacts were scored using the worst case scenario, illustrated by these examples of cyber incidents:

---

[7] Other examples of cyber incidents that would likely have impacts across all of the other risk impact areas include:

- The 2012 virus attack on Saudi Aramco did not directly result in an operational impact, however 30,000 systems were infected. The virus deleted data from computer hard drives. An incident of this type would severely impact business operations, have financial consequences, and likely result in regulatory, statutory, or compliance review and scrutiny.
- The Lansing Board of Water and Light ransomware attack that impacted significant numbers of corporate computers. In that situation, an employee opened an email leading to the incident. Utility service delivery was not impacted.

[8] For example:

- The United States Office of Personnel Management (OPM) had a data breach of information records for 21.5 million people, possibly including background check information and fingerprints. This type of information compromise would have both Regulatory, Legal, and Compliance impacts and Financial impacts.
- The recent Yahoo password breach affecting 500 million accounts provides an example of two issues that could impact utility customers. A compromise of our customer passwords would expose customer personal information with resulting identity theft risks. In this case, there would likely be Regulatory, Legal, and Compliance, as well as Financial, impacts. Further, the Yahoo passwords could be the same passwords customers have used for their utility accounts. In this case, customer information would also be exposed to unauthorized access.

- **Operational and Reliability:** A score of 6 (Severe) was given to this risk. A cyber security incident impacting transmission and/or distribution of energy would directly impact the reliable delivery of energy.
- **Regulatory, Legal, and Compliance**: Cyber Security was scored a 5 (Extensive) in the Regulatory, Legal, and Compliance impact area. This is reasonable because a severe impact to operations would likely result in an extended and in-depth review of the incident, as well as the existing mitigations and activities related to Cyber Security at the time of the event.
- **Financial:** The Financial impact of a cyber security incident was also scored as a 5 (Extensive). A variety of cyber incidents could potentially result in this level of financial impact due to the high visibility of this kind of incident in our industry. A customer information breach may potentially result in reparations, security investigation and improvement costs, and a loss of customer confidence. An energy outage could result in financial impacts, loss of confidence, and/or increased insurance costs. The possibility of an incident destroying assets or data, such as an Advanced Meter Infrastructure (AMI) solution, could also be severe.

4.5 Explanation of Frequency Score

SMEs used empirical data to the extent available and/or their expertise to determine the likelihood of a cyber security incident score as a 4 (Occasional), which is defined in the REF as the possibility of a Cyber Security-related event occurring once every 3-10 years. Those assigning this score considered reports in open media, security research, information-sharing entities, contracted information services, and threat intelligence sources.

5 Baseline Risk Mitigation Plan[9]

As stated above, Cyber Security risk is a major cyber security incident that causes disruptions to electric or gas operations (e.g., SCADA system) or results in damage or disruption to the Companies' operations, reputation, or disclosure of sensitive data. The 2015 baseline mitigations discussed below include the current evolution of the Companies' risk 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' baseline mitigation plan for this risk consists of five types controls aligned with the control functions in NIST Cyber Security Framework noted above: (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover. SMEs from the Information Security department collaborated to identify and document them. These controls focus on safety-related impacts[10] (i.e., Health, Safety, and Environment) per guidance provided by the Commission in D.16-08-018,[11] as well as controls and

[9] As of 2015, which is the base year for purposes of this Report.
[10] The Baseline and Proposed Risk Mitigation Plans may include mandated, compliance-driven mitigations.
[11] 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."

mitigations that may address reliability.[12] Accordingly, the controls and mitigations described in Sections 5 and 6 primarily address safety-related impacts. Note that the controls and mitigations in the baseline and proposed plans are intended to address various Cyber Security events, not just the scenario used for purposes of risk scoring.

The control functions provide a framework for the activities and projects used to maintain the cyber security posture. Some sample activities and 2015 projects are discussed for each of the functional areas. Additional activities are also performed and projects implemented, which are not completely enumerated here due to the confidential nature of the cyber security function and mitigation strategies. Also, when technological capabilities are implemented, they are used as long as they continue to effectively mitigate the associated risks, so there are not necessarily projects in every functional area every year. In some cases, additional activities and projects are necessary to specifically address some mandates.

The benefits of the current baseline mitigation approach are that it has been active and maturing for several years with the corresponding improvements in risk identification, tracking, and mitigation. It has been integrated into business processes, technology projects, and the organizational culture. Because more people in the organization are security aware, more potential issues are addressed sooner so that risks can be avoided. Also, security is addressed earlier in the acquisition and development lifecycles.

Cyber Security has had consistent capital funding for several years as well. These projects have established a core set of control capabilities that are leveraged by business projects and ongoing operations.

1. Identify

Program activities in the Identify Function include maintaining a security policy framework, asset management, risk assessments, threat intelligence, and risk management. For example, in conjunction with the IT Enterprise Architecture group, the Information Security control capabilities are documented. Risk assessments conducted by internal and external resources review the security posture of practices, technology, security controls, and other business activities. The assessments identify opportunities for improvements. These opportunities are prioritized via the risk management process. As projects are identified, funded, and completed, the security capabilities are updated in the capability repository.

[12] Reliability typically has an impact on safety. Accordingly, it is difficult to separate reliability and safety.

2. Protect

Protection-oriented activities are focused on avoiding or limiting potential cyber security events. Activities in this functional area include: managing asset access, cyber security awareness and training, protective technologies, and system maintenance. Ongoing cyber security awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cyber security. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management, and supporting network protections, such as firewalls and intrusion detection and prevention.

In 2015, several projects were completed to support this functional area, including:

- An update and enhancement of security of endpoints, such as employee laptops. This project added advanced malware detection and other protections to avoid or reduce the impact of endpoint compromises.
- A rebuild of the public key infrastructure used to issue and manage certificates to authenticate devices, applications, and services. Cryptographic algorithms have a limited lifetime and must be updated periodically to maintain their effectiveness. This rebuild was partially driven by the need to replace an encryption algorithm, which was not considered resilient to current computer processors.
- The initiation of a data loss prevention capability to detect potentially unauthorized movement of information. The primary focus of this initial effort was the protection of customer information.

Non-GRC projects at SDG&E were also completed in the Protection area:

- Improvements on the communication infrastructure security; and
- Implementation of an isolated infrastructure to support NERC CIP security activities to minimize exposure to unrelated risks.

Note that because these projects were completed in 2015, they are reflected in the baseline risk mitigation plan, but will not continue for purposes of the proposed mitigation plan, discussed in Section 6. However, other projects for the Protect functional area are proposed and anticipated in the proposed plan.

3. Detect

The Detect Function enables timely discovery of Cyber Security events by monitoring security-related activities in systems and applications, anomaly detection, and security event detection and escalation. The 7x24 Security Operations Center monitors detection infrastructure systems to investigate security events. If the security events have the potential to impact the organization, they are escalated to the security incident response process.

4. Respond

The Respond Function supports the ability to contain the impact of a cyber security event. The response team coordinates cyber security incident response when a security event is escalated. They also provide analysis of the incident, during the incident, to determine the most effective response, as well as after the incident in terms of lessons learned. During the incident, communications with stakeholders are maintained. This functional area is the focus of ongoing training to maintain readiness through exercises to validate the response plans for high impact systems.

5. Recover

The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security event. This function is a core capability of the Information Technology business unit. The Information Security department's focus on Recovery functions is to maintain resilience against a Cyber Security event and, if necessary, to restore cyber security capabilities to a known state after an incident.

6 Proposed Risk Mitigation Plan

Planning the mitigation of Cyber Security risk is particularly challenging because of the wide range of potential risk drivers, including: rapid changes in technology, innovations in business capabilities, evolving threats in terms of sophistication, automation, and aggressiveness, and increasing system interdependencies. Cyber Security risk cannot be completely mitigated or avoided; however, the Companies can manage it by following well understood principles, recommending best practices, and striving to keep pace with changing threats.

The 2015 baseline mitigations outlined in Section 5 will continue to be performed in the proposed plan. However, due to the evolving nature of the threats associated with this risk, if only the baseline mitigations were to be maintained, the risk would likely grow. Accordingly, in addition to the baseline controls, there will be several, new capital projects to improve or replace existing security capabilities to address changing threats or supported technologies. Also, there is a proposed increase in on-site staff at SoCalGas, the introduction of an entry level staffing program, and use of external services for some solutions instead of internal resources.

The additional employees, located primarily in the SoCalGas facilities, will provide better business and IT project and operational support. Also, an Information Security Associates program is proposed to add more entry level staff at both Companies in order to support the transition of the aging workforce, as well as lowering the overall average employee cost. These incremental changes are further described below.

1. Identify
   - Compliance Records Management – implement a system of recordkeeping dedicated to compliance records to better support regulatory auditing and governance of required safety-related Cyber Security risk mitigation activity.
   - Enterprise Threat Intelligence – automate distribution of threat intelligence to business and system owners to improve Cyber Security risk awareness and engagement.

2. Protect
   - Web Applications and Database Firewalls – improve protective capabilities for web applications and databases to reduce the likelihood and impact of an incident.
   - Host Based Protection – improve host-based protections for direct attacks and to help prevent attackers from pivoting to a host from a neighboring host.

3. Detect
   - Insider Threat Detection/Prevention – leverage emerging technologies to improve the detection of insider threat activities and the related risk impacts.
   - Perimeter Tap Infrastructure Redesign – improve the performance and visibility into network traffic to limit impacts of incidents.

4. Respond
   - Incident Response Secure Collaboration – implement a secure, out-of-band communication capability to coordinate and support incident response activity.
   - Security Orchestration – automate and support enhancements to the workflow related to responding to and analyzing escalated events to better manage and learn from cyber events.

5. Recover
   - Information Security technology backup and recovery – refresh backup and recovery for sensitive information security systems so as to return to a safe and secure risk posture.

7 Summary of Mitigations

Table 4a and 4b summarize the 2015 baseline risk mitigation plans, the risk driver(s) a control addresses, and the 2015 baseline costs for Cyber Security risk for SDG&E and SoCalGas, respectively. 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 these tables were estimated using assumptions provided by SMEs and available accounting data.

Mitigation costs include capital costs for new and updated infrastructure, as well as operating and maintenance costs for labor resources and non-labor expenses. The costs represented here are the initial costs of the baseline mitigations before they are reallocated between SDG&E and SoCalGas. In general, capital costs are allocated to SoCalGas, and O&M costs are allocated to SDG&E. Non-GRC costs are those supporting mandated NERC CIP compliance. Only SDG&E has non-GRC costs, and none of these costs are shared with SoCalGas.

Table 4a: SDG&E Baseline Risk Mitigation Plan[13]
(Direct 2015 $000)[14]

ID	Control	Risk Drivers Addressed	Capital[15]	O&M	Control Total[16]	GRC Total[17]
1	Identify*	Addresses all risk drivers by defining the foundational asset and risk information necessary for mitigation	n/a	$1,420	$1,420	$780
2	Protect*	Address all risk drivers via controls, training, and activities focused on preventing or minimizing impacts	1,820	2,880	4,700	3,870
3	Detect*	Address all risk drivers by monitoring, detecting, and analyzing cyber events	0	1,020	1,020	880
4	Respond*	Address all risk drivers by containing and remediating cyber incidents	n/a	810	810	620
5	Recover*	Address all risk drivers by planning	n/a	70	70	20

[13] Recorded costs were rounded to the nearest $10,000.
[14] The figures provided in Table 4a, 4b, 5a, and 5b 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.
[15] 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.
[16] 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).
[17] The GRC Total column shows costs typically presented in a GRC.

ID	Control	Risk Drivers Addressed	Capital[15]	O&M	Control Total[16]	GRC Total[17]
		and communicating the restoration of services after an incident				
	TOTAL COST		$1,820	$6,200	$8,020	$6,170

***** Includes one or more mandated activities

Table 4b: SoCalGas Baseline Risk Mitigation Plan[18]
(Direct 2015 $000)

ID	Control	Risk Drivers Addressed	Capital[19]	O&M	Control Total[20]	GRC Total[21]
1	Identify	Addresses all risk drivers by defining the foundational asset and risk information necessary for mitigation	n/a	$50	$50	$50
2	Protect	Address all risk drivers via controls, training, and activities focused on preventing or minimizing impacts	6,370	400	6,770	6,770
3	Detect	Address all risk drivers by monitoring, detecting, and analyzing cyber events	n/a	n/a	n/a	n/a
4	Respond	Address all risk drivers by containing and remediating cyber incidents	n/a	10	10	10
5	Recover	Address all risk drivers by planning and communicating the restoration of services after an incident	n/a	n/a	n/a	n/a
	TOTAL		$6,370	$460	$6,830	$6,830

[18] Recorded costs were rounded to the nearest $10,000.
[19] 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.
[20] 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).
[21] The GRC Total column shows costs typically presented in a GRC.

ID	Control	Risk Drivers Addressed	Capital[19]	O&M	Control Total[20]	GRC Total[21]
	COST					

***** Includes one or more mandated activities

The baseline costs above in Tables 4a and 4b reflect the actual Information Security O&M and Capital costs based on accounting data.

The Companies have established a core set of control capabilities that are leveraged by business projects and ongoing operations. In 2015, there were no capital projects within the functional controls of Identify, Detect, Respond and Recover.

Table 5a and 5b summarize the proposed mitigation plans, associated projected ranges of estimated O&M expenses for 2019, and projected ranges of estimated capital costs for the years 2017-2019 for SDG&E and SoCalGas, respectively. It is important to note that the Companies are identifying potential ranges of costs in this plan, and is not requesting funding approval. The Companies will request approval of funding, in its 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 5a and 5b, the Companies are using a 2019 forecast provided in ranges based on 2015 dollars.

Table 5a: SDG&E Proposed Risk Mitigation Plan[22]
(Direct 2015 $000)

ID	Mitigation	Risk Drivers Addressed	2017-2019 Capital[23]	2019 O&M	Mitigation Total[24]	GRC Total[25]
1	Identify*	Addresses all risk drivers by defining the foundational asset and risk information necessary for mitigation	n/a	$1,100 - 1,570	$1,100 - 1,570	$460 - 720
2	Protect*	Address all risk drivers via controls, training, and activities focused on preventing or minimizing impacts	3,000 - 9,000	4,000 - 6,020	7,000 - 15,020	6,170 - 14,130
3	Detect*	Address all risk drivers by monitoring, detecting, and analyzing cyber events	n/a	1,280 - 1,630	1,280 - 1,630	1,140 - 1,340
4	Respond*	Address all risk drivers by containing and	n/a	940 - 1,500	940 - 1,500	740 - 1,150

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

		remediating cyber incidents				
5	Recover*	Address all risk drivers by planning and communicating the restoration of services after an incident	n/a	250 - 450	250 - 450	200 - 340
	TOTAL COST		$3,000 - 9,000	$7,570 - 11,170	$10,570 - 20,170	$8,710 - 17,680

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

Table 5b: SoCalGas Proposed Risk Mitigation Plan[26]
(Direct 2015 $000)

ID	Mitigation	Risk Drivers Addressed	2017-2019 Capital[27]	2019 O&M	Mitigation Total[28]	GRC Total[29]
1	Identify	Addresses all risk drivers by defining the foundational asset and risk information necessary for mitigation	$0 - 7,500	$110 - 560	$110 - 8,060	$110 - 8,060
2	Protect	Address all risk drivers via controls, training, and activities focused on preventing or minimizing impacts	28,700 - 41,300	400 - 1,060	29,100 - 42,360	29,100 - 42,360
3	Detect	Address all risk drivers by monitoring, detecting, and analyzing cyber	9,450 - 14,900	0 - 150	9,450 - 15,050	9,450 - 15,050

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

		events				
4	Respond	Address all risk drivers by containing and remediating cyber incidents	7,000 - 12,000	10 - 160	7,010 - 12,160	7,010 - 12,160
5	Recover	Address all risk drivers by planning and communicating the restoration of services after an incident	0 - 6,000	n/a	0 - 6,000	0 - 6,000
	TOTAL COST		$45,150 - 81,700	$520 - 1,930	$45,670 - 83,630	$45,670 - 83,630

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

Capital cost estimates are based on the current Information Security project roadmap. Depending on other budget priorities, some projects may be implemented in later years. The low range is based on the roadmap timelines. The high range for the capital projects includes costs for projects from previous years being completed in that year, and projects that are identified and prioritized during the risk assessment process.

O&M costs have a labor and a non-labor component. The estimated labor costs are based on 2015 costs as the low range plus a minimal number of Information Security Associates (discussed in the benefits section below). The high range includes additional full-time staff to support the Companies' projects and operations, and other activities identified in risk assessments.

The non-labor component of the O&M costs is estimated by escalating costs associated with supporting the capital projects after their implementation. The high range also accommodates the costs of addressing capability improvements utilizing service-based offerings where there is a rate benefit and appropriate risk management.

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.[30] 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.[31]

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.

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.

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

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.[32] 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.

8.1.2 Calculating Risk Spend Efficiency

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 Tables 5a and 5b 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

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

The NIST developed a cyber security framework to serve as an implementation guide for corporate countermeasures. In this framework, core activities and outcomes are placed into five functions: identify, protect, detect, respond, and recover. The Company has measures that address requirements under these functions.

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

The migration activities (within the five functional control areas) were combined and assessed as one aggregated mitigation for the risk reduction analysis. Because cyber threats are in a constant evolutionary state, corporate countermeasures also evolve over time and, generally are lagging. Since countermeasures are designed to match known threats, all of them are categorized as baseline, so only one set of security measures was analyzed. The methodology used to estimate risk reduction was based on internal self-assessment results and the judgment of SMEs. This analysis addresses the mitigations at both utilities, collectively.

As self-assessments are performed over time, progress on each of the functions is noted. If the baseline portfolio were to not be funded, it can be assumed that risk would revert to an earlier state. This is the principle that is used in the estimation of risk reduction from this mitigation; namely that the benefit is the difference in performance between the current state and an earlier, known state.

Year 2015 assessment results are used to define the earlier, known state, and 2016 assessment results are used to define the current posture. Assessment results are given in units consistent with the 7X7 matrix of the risk evaluation framework. Because results are given for each of the five cyber security functions, and not for the full cyber security portfolio, it is necessary to consolidate them into a single value. Also, the functions were assigned weights that reflected the relative contribution of each to overall benefits, SMEs assigned determined these assignments as shown in Figure :

Figure 3: Control Functions - Contribution to Overall Benefits

Function	Contribution to overall benefits
Identify	15%
Protect	15%
Detect	20%
Respond	20%
Recover	30%

Applying these weights, SMEs estimated that the remaining risk is 35% of the original risk from the earlier, known state. This means 65% of the risk is estimated to have been mitigated. This is a conservative result because security measures existed before the year 2015.

8.3 Risk Spend Efficiency Results

Figures 4 and 5display the range[33] of RSEs for Cyber Security risk for SoCalGas and SDG&E.

[33] Based on the low and high cost ranges provided in Tables 5a and 5b of this chapter.

Figure 4: SoCalGas Risk Spend Efficiency

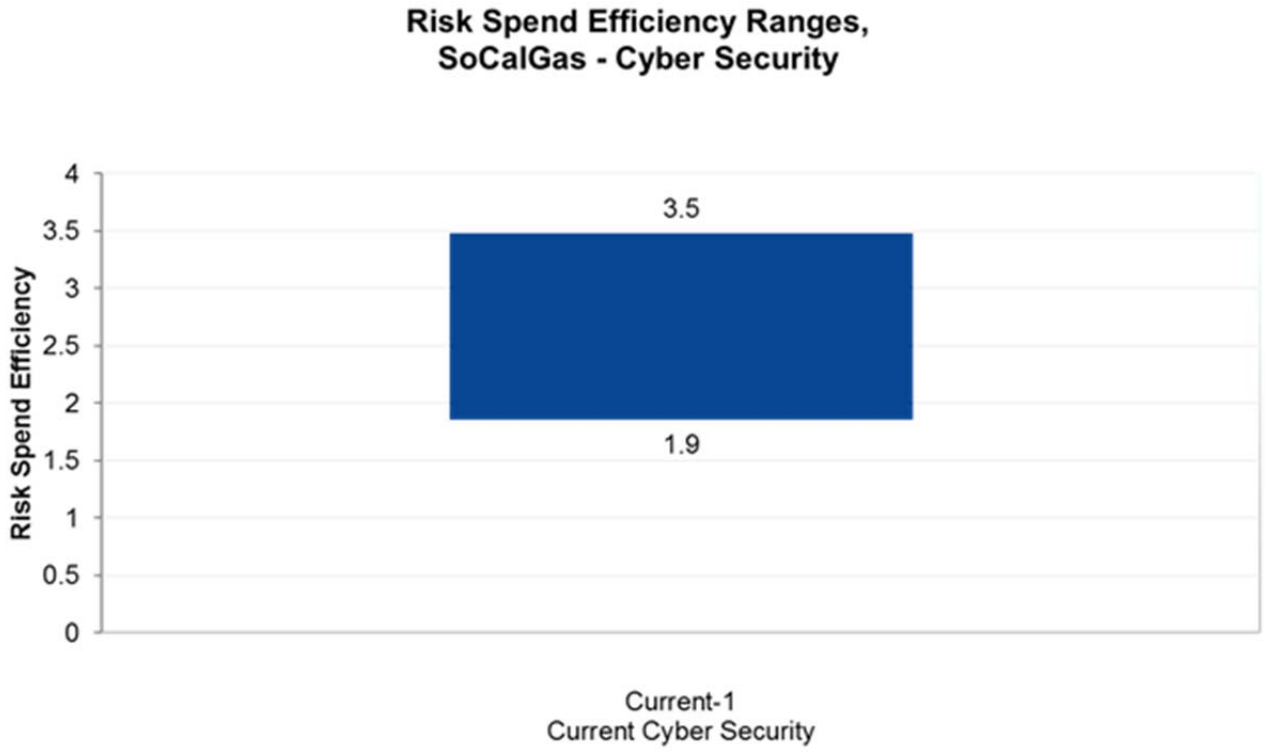
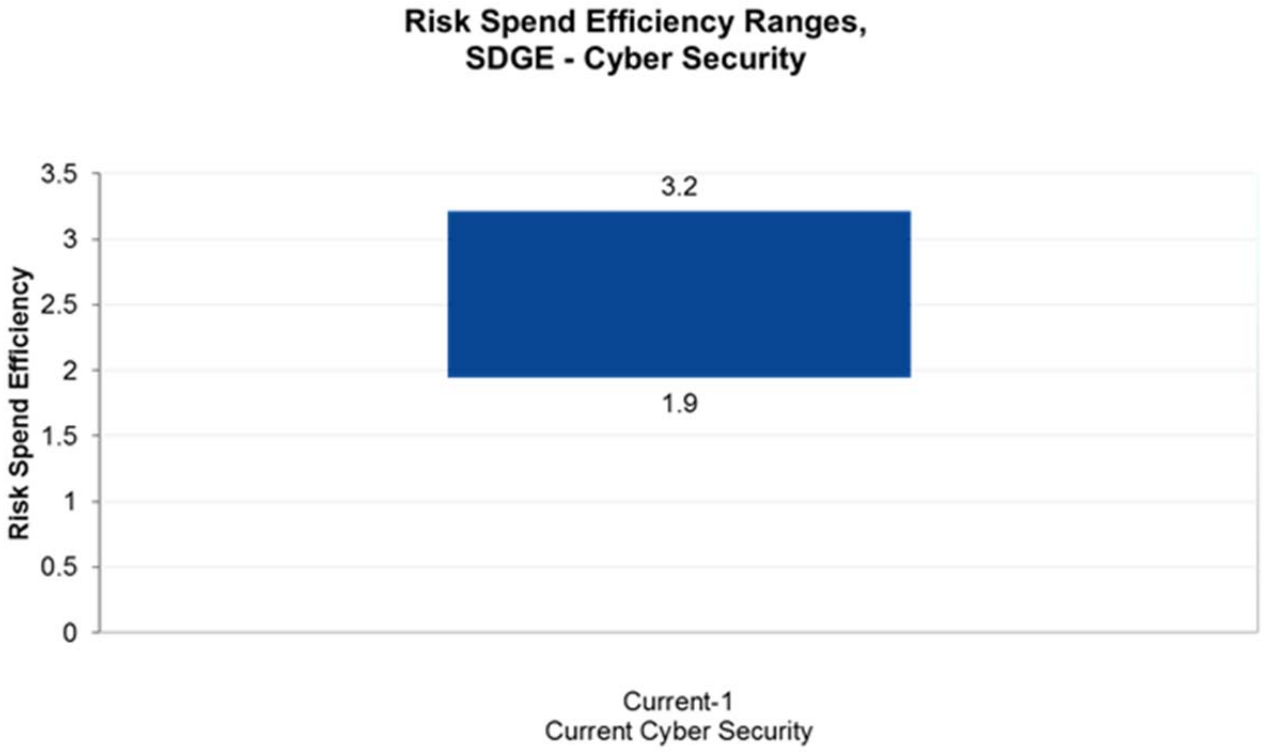


Figure 5: SDG&E Risk Spend Efficiency



9 Alternatives Analysis

The Companies considered alternatives to the proposed mitigations as it developed the proposed mitigation plan for the Cyber Security 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.

9.1 Alternative 1 – Address All Known Issues

The first alternative considered was to more aggressively mitigate risk by quickly addressing all known issues. If the organization is less risk tolerant, then the Information Security program will address more of the medium and low risks more aggressively, reducing windows of vulnerability and addressing identified control capability risks sooner.

More aggressively addressing risk would increase capital spending, maintenance costs, and staffing in order to implement and operate more cyber security controls in a shorter period of time. Also, a more aggressive approach would lead to more business function-specific solutions instead of enterprise

solutions, also increasing the cost of ownership. The amount of the cost increase depends on the degree of the accelerated activity. An increase in capital project costs also has a longer-term increase in labor and non-labor O&M costs in future years.

This alternative was dismissed in favor of the proposed plan due to resource, financial, and affordability constraints. The proposed plan balances resources and affordability by prioritizing projects and programs rather than addressing all known issues, while also reducing potential risk exposure to the extent it is feasible.

9.2 Alternative 2 – Delay Security Capability Implementation

The second alternative that was considered was to delay security capability implementation in response to a cyber threat, and business and Cyber Security technology changes. If the organization had a higher risk tolerance, then the Information Security program would slow down the implementation of security controls and focus on a smaller set of risks and business areas, increasing overall risk exposure.

Moderating the Cyber Security risk management would reduce capital spending and maintenance costs, as well as reduce increased staffing requirements. The amount of the decrease in cost would depend on the amount of moderation.

The Companies believe their risk management culture does not allow for this approach given the commitments to safety and cyber security. The current potential drivers of increasing capabilities of threat agents and higher risk exposure due to innovative technologies are increasing the Companies' risk. Only moderating cyber security activities and spending would not be beneficial to customers with respect to safe and reliable energy delivery and protecting sensitive customer information.