Company:	Southern California Gas Company (U 904 G)
Proceeding:	2019 General Rate Case
Application:	A.17-10-008
Exhibit:	SCG-27-R

REVISED

SOCALGAS

DIRECT TESTIMONY OF GAVIN WORDEN

(CYBERSECURITY)

DECEMBER 2017

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

SoCalGas
A Sempra Energy utility®

TABLE OF CONTENTS

LIST OF APPENDICES

SUMMARY

CYBERSECURITY (In 2016 $)			
	2016 Adjusted-Recorded (000s)	TY 2019 Estimated (000s)	Change (000s)
Total Non-Shared Services	0	0	0
Total Shared Services (Incurred)	238	708	470
Total O&M	**238**	**708**	**470**

CYBERSECURITY (In 2016 $)				
	2016 Adjusted-Recorded (000s)	Estimated 2017 (000s)	Estimated 2018 (000s)	Estimated 2019 (000s)
Total CAPITAL	**0**	**17,844**	**19,476**	**22,731**

Summary of Requests

- Provide cybersecurity support services that directly contribute to Southern California Gas Company's (SoCalGas) ability to provide secure, safe, and reliable service at reasonable rates for our customers while maintaining a safe work environment for our employees by managing cybersecurity risk.
- The cybersecurity risk involves a major cybersecurity incident that causes disruptions to electric or gas operations (*e.g.*, supervisory control and data acquisition (SCADA) system) or results in damage or disruption to Company operations, reputation, or disclosure of sensitive data. Our mitigation plan is based on the National Institute of Standards and Technology's Cybersecurity Framework[1] (NIST CSF or Framework), which was developed in response to Executive Order 13636 of February 21, 2013, titled "Improving Critical Infrastructure Cybersecurity."[2]
- The request includes operations and maintenance (O&M) labor costs to support cybersecurity practices and capital and O&M non-labor costs to implement and maintain technology-based cybersecurity controls.

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

[2] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity and https://www.dhs.gov/publication/eo-13636-ppd-21-fact-sheet.

- Enhance and update cybersecurity infrastructure to minimize the likelihood and impact of ever-changing security threats disrupting business operations and to secure customer data to meet growing privacy regulations.
- Position the Cybersecurity Department to support the continued utilization of technology innovations to enhance the customer experience, increase system capabilities, and gain operational efficiencies by identifying and proactively mitigating cybersecurity risks.

REVISED SOCALGAS DIRECT TESTIMONY OF GAVIN WORDEN
CYBERSECURITY

I. INTRODUCTION

A. Summary of Cybersecurity Costs and Activities

My testimony supports the Test Year (TY) 2019 forecasts for O&M costs for shared services, and capital costs for the forecast years 2017, 2018, and 2019, associated with the Cybersecurity area for SoCalGas. Table GW-1 below summarizes my sponsored costs.

TABLE GW-1

Test Year 2019 Summary of Total Costs

CYBERSECURITY (In 2016 $)			
	2016 Adjusted-Recorded (000s)	TY 2019 Estimated (000s)	Change (000s)
Total Non-Shared Services	0	0	0
Total Shared Services (Incurred)	238	708	470
Total O&M	**238**	**708**	**470**

CYBERSECURITY (In 2016 $)				
	2016 Adjusted-Recorded (000s)	Estimated 2017 (000s)	Estimated 2018 (000s)	Estimated 2019 (000s)
Total CAPITAL	**0**	**17,844**	**19,476**	**22,731**

The Cybersecurity Department (formerly the Information Security Department) is responsible for cybersecurity risk management of the information and operational technologies for SoCalGas, San Diego Gas and Electric Company (SDG&E), and Sempra Energy Corporate Center (Corporate Center). Cybersecurity risk management is performed through activities and using technical controls built upon the NIST CSF five core Functions of Identify, Protect, Detect, Respond, and Recover. The services provided by the Cybersecurity Department are focused on maintaining and improving the Company's security posture in an environment of increasing threat capabilities. The Cybersecurity Department supports technology innovations and enhancements within the business by reducing both the likelihood and potential impact of cybersecurity incidents to all business areas within SoCalGas, SDG&E, and Corporate Center while balancing costs and applying prioritized risk management. Additionally, the Cybersecurity Department's activities support enterprise cybersecurity capabilities and provide cybersecurity technical support and training to other business and informational technology (IT) groups so that they can perform their functions safely, reliably, and securely.

My testimony describes the cybersecurity risks, our approach for managing these risks, and the Cybersecurity Department's activities and costs associated with cybersecurity risk management. Other business areas may also have costs related to their cybersecurity risk management responsibilities and activities.

Cybersecurity is a shared service for SoCalGas, SDG&E, and Corporate Center and the costs set forth in my testimony are allocated between the Companies based on the mechanisms described in the testimony of Christopher Olmsted (Exhibit (Ex.) SCG-26). The cybersecurity risk management activities set forth in my testimony correspondingly benefit SoCalGas, SDG&E, and Corporate Center. The primary cost drivers for the cybersecurity costs discussed below are the addition of more on-site staff to provide cybersecurity expertise to SoCalGas implementation and development projects, replacing aging or obsolete cybersecurity control technology, adding new technical capabilities to address evolving threat capabilities and innovative technologies implemented by other business units, and increasing costs to maintain and support cybersecurity technologies. The costs have been categorized based on the activities and technical controls defined in the industry standard NIST CSF framework's Functional areas.

In addition to sponsoring my own organization's costs, my testimony also supports the costs associated with the Fueling Our Future (FOF) program's cybersecurity-related capital projects.

B. Summary of Risk Assessment Mitigation Phase-Related Costs

Certain costs supported in my testimony are driven by activities described in SoCalGas and SDG&E's November 30, 2016 Risk Assessment Mitigation Phase (RAMP) Report.[3] The RAMP Report presented an assessment of the key safety risks of SoCalGas and SDG&E and proposed plans for mitigating those risks. As discussed in the testimony of Diana Day and Jamie York (Ex. SCG-02/SDG&E-02), the costs of risk-mitigation projects and programs were translated from the RAMP Report into general rate case (GRC) individual witness areas.

[3] Investigation (I.) 16-10-016, Risk Assessment and Mitigation Phase Report of San Diego Gas & Electric Company and Southern California Gas Company, November 2016 (RAMP Report).

While preparing my GRC forecasts, I continued to evaluate the scope, schedule, resource requirements, synergies of RAMP-related projects and programs and alternative mitigations. Therefore, the final representation of RAMP costs may differ from the ranges shown in the original RAMP Report.

Table GW-2A and GW-2B provide a summary of the RAMP-related costs supported by my testimony by RAMP risk:

TABLE GW-2A

Summary of RAMP O&M Related Costs

CYBERSECURITY (In 2016 $)			
RAMP Report Risk Chapter	**2016 Embedded Base Costs (000s)**	**TY 2019 Estimated Incremental (000s)**	**Total (000s)**
SCG-3 Cyber Security	238	470	708
Total O&M	**238**	**470**	**708**

TABLE GW-2B

Summary of RAMP Capital Related Costs

CYBERSECURITY (In 2016 $)				
RAMP Risk Chapter	**2016 Embedded Base Costs (000s)**	**Estimated 2017 (000s)**	**Estimated 2018 (000s)**	**Estimated 2019 (000s)**
SCG-3 Cyber Security	0	17,844	19,476	22,731
Total Capital	**0**	**17,844**	**19,476**	**22,731**

C. Summary of Costs Related to Fueling our Future

As described in the testimony of Hal Snyder (Ex. SCG-03), SoCalGas and SDG&E kicked off the Fueling Our Future (FOF) initiative in May 2016 to identify and implement efficient operations improvements. The Cybersecurity Department will undertake two FOF initiatives. The two FOF capital projects are the Converged Perimeter Systems and Host Based Protection projects. These FOF projects are discussed in more detail in Section V below and the associated costs are summarized in Table GW-3 below.

TABLE GW-3

Summary of FOF Costs

Project Name	Description	Core Mitigation Function	2017 Estimated (000s)	2018 Estimated (000s)	TY 2019 Estimated (000s)
Converged Perimeter Systems	Fueling Our Future Idea #760	Protect	$2,516	$1,270	$0
Host Based Protection	Fueling Our Future Idea #790	Protect	$2,266	$23	$0

D. Organization of Testimony

My testimony is organized as follows:

- Section II provides a summary of SoCalGas and SDG&E's RAMP, defines cybersecurity risk, provides background on the Cybersecurity Program, discusses the Company's cybersecurity strategy and risk management process, and sets forth SoCalGas' safety culture.
- Section III states that SoCalGas has no the non-shared cybersecurity costs.
- Section IV provides the shared O&M costs.
- Section V presents the planned capital projects.
- Section VI concludes with a recap of my requests.
- Section VII sets forth my witness qualifications.

E. Risk Assessment Mitigation Phase

The majority of costs sponsored by my testimony are linked to managing cybersecurity risk, which is a top safety risk that was identified in the RAMP Report and is further described in the table below:

TABLE GW-4

RAMP Risks Associated with this Testimony

RAMP Risk	Description
Cybersecurity	This risk is a major cybersecurity 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.

In developing my request, priority was given to this key safety risk to determine which currently established risk control measures were important to continue and what incremental efforts were needed to further mitigate these risks. The Cybersecurity Program, described in detail below, continually reassesses current mitigating control activities versus best practices and threats created by continually evolving threat actor capabilities and increasing use of innovative technologies within the business. In addition to safety risks, the Cybersecurity Program addresses other risk area impacts such as operations, compliance, and financial with cybersecurity risk management controls and activities. The cybersecurity risk mitigations are designed to address as many business services and systems as possible. Most activities and projects discussed in this testimony support RAMP. In the following discussions, any of the activities and projects which do not support the mitigation of the RAMP cybersecurity risks are identified when they are described.

The general treatment of RAMP forecasting is described in the testimony of Diana Day (Ex. SCG-02/SDG&E-02). There are also a few instances where, in the course of developing my GRC forecast, additional safety-related mitigation activities were identified that were not included in the RAMP Report. These have been marked as RAMP-Post Filing and treated as if they had been included in the original RAMP Report.

For each of these risks, an embedded 2016 cost-to-mitigate and any incremental costs expected by TY 2019 are shown in Tables GW-5A and GW-5B below. RAMP-related costs are further described in Sections III, IV, and V below as well as in my workpapers.

TABLE GW-5A

Summary of RAMP O&M-Related Costs

CYBERSECURITY (In 2016 $)			
RAMP Report Risk Chapter	**2016 Embedded Base Costs (000s)**	**TY 2019 Estimated Incremental (000s)**	**Total (000s)**
SCG-3 Cyber Security	238	470	708
Total O&M	**238**	**470**	**708**

TABLE GW-5B

Summary of RAMP Capital-Related Costs

CYBERSECURITY (In 2016 $)				
RAMP Report Risk Chapter	**2016 Embedded Base Costs (000s)**	**Estimated 2017 (000s)**	**Estimated 2018 (000s)**	**Estimated 2019 (000s)**
SCG-3 Cyber Security	0	17,844	19,476	22,731
Total Capital	**0**	**17,844**	**19,476**	**22,731**

While the starting point for consideration of the risk mitigation effort and cost was the RAMP Report, SoCalGas' evaluation of those efforts was on-going in preparation of this GRC request and consideration of alternative mitigations. Changes in scope, schedule, availability of resources, overlaps or synergies of mitigation efforts, and shared costs or benefits were also considered. Therefore, the incremental costs of risk mitigation sponsored in my testimony may differ from those first identified in the RAMP Report. Significant changes to those original cost estimates are discussed further in my testimony or workpapers related to that mitigation effort. My incremental request supports the on-going management of these risks that could pose significant safety, reliability, and financial consequences to our customers and employees. The anticipated risk reduction benefits that may be achieved by the incremental request set forth in my testimony are all associated with reducing cybersecurity risk.

1. Cybersecurity Risk

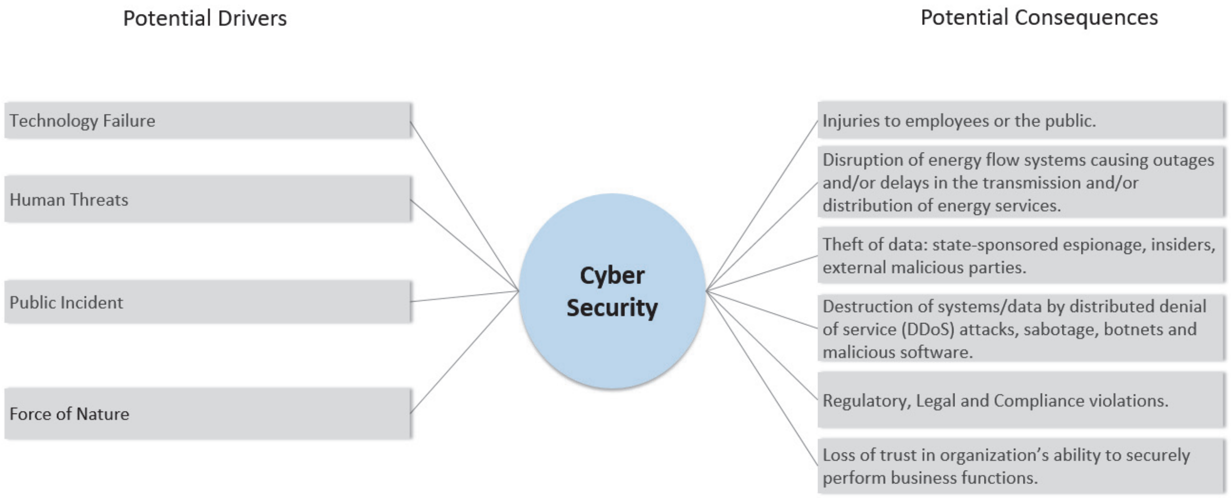
Cybersecurity risk involves a major cybersecurity incident that causes disruptions to electric or gas operations (*e.g.*, SCADA system) or results in damage or disruption to company operations, reputation, or disclosure of sensitive data.

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, 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 cybersecurity risk is a documented concern at the national and international level, as described in the following sections.

a. Potential Drivers

When performing its cybersecurity risk assessment, the Company relied on the risk "bow tie," shown in the figure below, which 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 potential drivers and consequences described below.

Figure GW-1: Risk Bow Tie


Potential Drivers
Potential Consequences
Technology Failure
Human Threats
Public Incident
Force of Nature
Cyber Security
Injuries to employees or the public.
Disruption of energy flow systems causing outages and/or delays in the transmission and/or distribution of energy services.
Theft of data: state-sponsored espionage, insiders, external malicious parties.
Destruction of systems/data by distributed denial of service (DDoS) attacks, sabotage, botnets and malicious software.
Regulatory, Legal and Compliance violations.
Loss of trust in organization's ability to securely perform business functions.

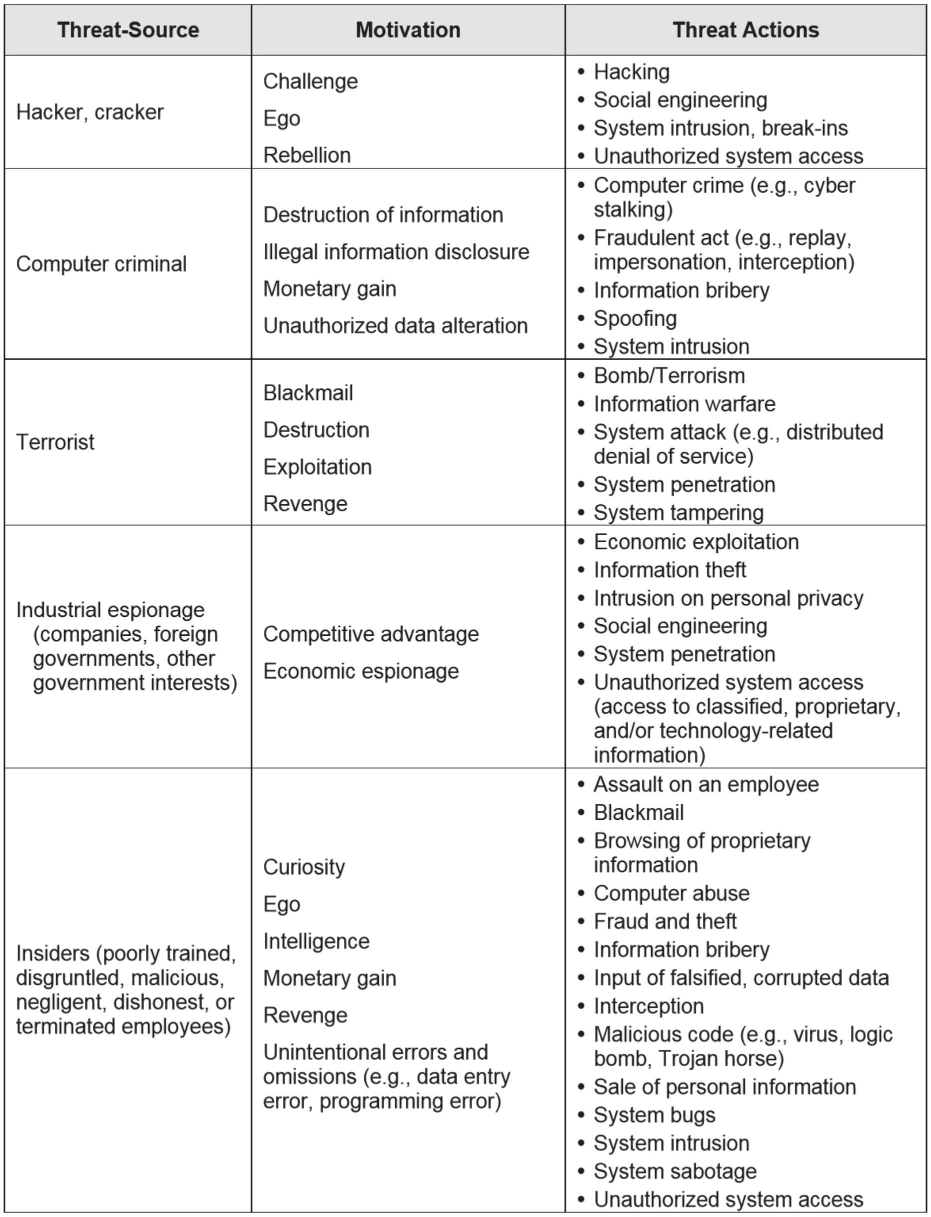
The potential drivers, or potential indicators of risk, include, but are not limited to:

- Technology Failure – The malfunction or failure of a technological device.
- 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 as are described in Table GW-6 below.

Table GW-6

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 deliberate human 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 IV and V below, to protect their business interests, employees, contractors, customers, and the public.

b. 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, may 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, criminal organizations, and other 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 cybersecurity 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 (*e.g.*, an incident of non-compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (Federal Energy Regulatory Commission (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 cybersecurity incidents, technologically interact with partners, and retain employees.

- o Customer level impacts may make it difficult to collect necessary customer information and conduct other interactions, tainted by an unwillingness to share information.

Cybersecurity threats are dynamic and new adversarial techniques may evade current cybersecurity controls, rendering them obsolete and ineffective. Technology innovations and adoption thereof continually increase the exposure of infrastructure and business services to a risk impact.

2. Cybersecurity Program

The Cybersecurity Department is responsible for the identification and management of cybersecurity risks for SoCalGas, SDG&E, and Corporate Center. This Cybersecurity Program overview presents the cybersecurity risks addressed by the costs described in my testimony, the strategy followed, and the practices and controls used to manage the identified risks. Cybersecurity is a cross-cutting risk because an incident could potentially impact several areas throughout the Companies in many different ways.

The Cybersecurity Program focuses on responding to and mitigating potential drivers, and the potential resulting events of which the company is aware. The Company also strives to implement mitigations to address those instances (drivers and/or events) that may be unknown to the Company. The mitigation approach leverages a framework of cybersecurity controls across the enterprise, with an 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.

3. Cybersecurity Strategy

The Company's cybersecurity risk management strategy is based on a set of business and cybersecurity-oriented guiding principles, which aligns with the enterprise risk management strategy to ensure that cybersecurity risk is evaluated and managed in a manner that is consistent with the organization's overall objectives and strategy. The cybersecurity risk management strategy includes: 1) a risk monitoring strategy, which defines the processes used to monitor and communicate cybersecurity risks and the maturity and efficacy of the Cybersecurity Program over time; 2) a governance program that defines the structure and organization of the Cybersecurity Program and the approach to provide oversight and governance for cybersecurity activities; and 3) a risk management framework, which defines the practices, procedures, and controls applied to managing cybersecurity risks.

The goals of the cybersecurity risk management strategy are to secure critical infrastructure, secure sensitive business information assets and critical business operations, enhance the maturity of the Cybersecurity Program, and ensure that cybersecurity is an integral part of the Company's culture. The strategy is particularly focused on enhancing defensive capabilities, increasing protection of critical and other high-risk assets, ensuring compliance with legal and regulatory requirements and privacy standards and practices, and collaborating with and learning from others.

In support and furtherance of the cybersecurity risk management strategy goals, the Companies continuously cycle through the following activities:

- Identify and prioritize business functions, as well as the critical or high-risk assets/systems within those functions, based on cybersecurity risk impact assessments.
- Utilize practices and controls to manage potential risk impacts of threats and vulnerabilities.
- Periodically assess the completeness and effectiveness of the Cybersecurity Program's practices and controls.
- Prioritize and implement enhancement activities to reduce identified risks.

The cybersecurity risk management strategy is implemented by prioritized risk mitigation using assessments, testing, and reliable intelligence. Solutions are based on best practices and are applicable across the enterprise and automated, if possible. The goal is to maintain or reduce the current risk posture with respect to escalating threats and an increasing attack surface due to technological innovations in customer, partner, and business capabilities.

4. Cybersecurity Risk Management

The Company's cybersecurity risk management process prioritizes resources to address identified risks. The Cybersecurity Program governs the risk management activities through the application of best practices, acceptable use policies, security standards, and technology requirements for managing and maintaining technology systems.[4] Risks are identified using

[4] In Application (A.) 15-05-004, the Safety Model Assessment Proceeding (S-MAP), SoCalGas provided the supporting testimony of Scott King, which described the Cybersecurity Program and the cybersecurity risk management process.

multiple sources of information and assessments of risk mitigation practices and critical cybersecurity controls, which are mapped to the NIST CSF to provide a programmatic summary. The NIST CSF is the current foundational document used as the cybersecurity risk management framework.[5] Efforts to manage risk are prioritized based on risk scoring, benefits of the control activity, and evolving threats to the safety and reliability of critical systems.

Managing cybersecurity risk is a key business practice at the Company that continually evolves to keep pace with threats, technology innovations, and advances in cybersecurity best practices to efficiently and cost-effectively manage cyber-related risks. In addition to the Cybersecurity Department, several other departments throughout the Company have a role in supporting risk management activities. The NIST CSF is used to group cybersecurity risk mitigation plan activities and projects into the five core Functions described below. The cybersecurity costs presented in Sections IV and V below use the Framework.

In response to Executive Order 13636, the NIST CSF was developed through collaboration between the Federal Government and the private sector to address and manage cybersecurity risk cost-effectively based on business needs. The NIST CSF supports the application of cybersecurity risk controls and best practices to reduce and manage cybersecurity risks in order to improve the security and resilience of critical infrastructure. Effective industry practices from multiple resources have been grouped into five core Functions, which are the

[5] *See* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (February 12, 2014) (NIST CSF) https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (includes mappings to NIST SP 800-53r4 and CSC 20). *See also* Joint Task Force Transformation Initiative, NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (NIST SP 800-53r4) http://dx.doi.org/10.6028/NIST.SP.800-53r4 (provides a compendium of security and privacy controls based on asset related risks); Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense (CSC 20) Version 6.0 (October 15, 2015) (describes 20 controls recommended for implementation along with associated descriptions of associated practices and suggested approaches for implementing controls); U.S. Department of Energy and U.S. Department of Homeland Security, Cybersecurity Capability Maturity Model (C2M2) Version 1.1 (February 2014) (defines 10 domains of cybersecurity practices with practice maturity attributes. Versions for the Electric Sector, Oil and Natural Gas Sectors, and a general version for other parts of the organization. Includes self-assessment tools to determine an organization's maturity level); U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance (January 2015) (describes approaches for implementing the NIST CSF with or without the C2M2 approach).

main components of the Framework: (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover. The definitions and descriptions of the functions are described below.[6]

Identify

Identify refers to developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the NIST CSF. Understanding the business context, the resources that support critical functions, and the related cybersecurity 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.[7]

Program activities in the Identify Function include maintaining a security policy framework, asset management, risk assessments, threat intelligence, and risk management. For example, cybersecurity control capabilities are documented in conjunction with the IT Enterprise Architecture group. 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, which are prioritized via the risk management process. As projects are identified, funded, and completed, the security capabilities are updated in the capability repository.

Protect

Protect refers to developing and implementing 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 cybersecurity 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.[8]

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity

[6] NIST CSF at 8-9.
[7] NIST CSF at 8.
[8] NIST CSF at 8.

awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. 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.

Detect

Detect refers to developing and implementing appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of control Categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.[9]

Timely discovery of cybersecurity events is enabled by monitoring security-related activities in systems and applications, anomaly detection, and security event detection and escalation. The Information Security Operations Center monitors detection infrastructure systems to investigate security events 24 hours a day, 7 days a week. If the security events have the potential to impact the organization, they are escalated to the security incident response process.

Respond

Respond refers to developing and implementing appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.[10]

The Incident Response team coordinates cybersecurity incident response activities when a security event is escalated. During an incident, they maintain communications with stakeholders and provide analysis to determine the most effective response. The Incident Response team also analyzes the incident afterwards in terms of lessons learned. This functional area is the focus of ongoing training to maintain readiness through exercises to validate the response plans for high impact systems.

[9] NIST CSF at 8.

[10] NIST CSF at 8-9.

Recover

Recover refers to developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of control Categories within this Function include Recovery Planning, Improvements, and Communications.[11]

The Recover Function is a core capability of the Information Technology. The Cybersecurity Department's focus on recovery functions is to maintain resilience against a cybersecurity event and, if necessary, to restore cybersecurity capabilities to a known state after an incident.

The control Categories within each of the five core Functions are described in Table GW-7 below.

Table GW-7

NIST CSF Category Descriptions

Function Name	Category Name	Category Description
IDENTIFY	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
IDENTIFY	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
IDENTIFY	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
IDENTIFY	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
IDENTIFY	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT	Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
PROTECT	Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
PROTECT	Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

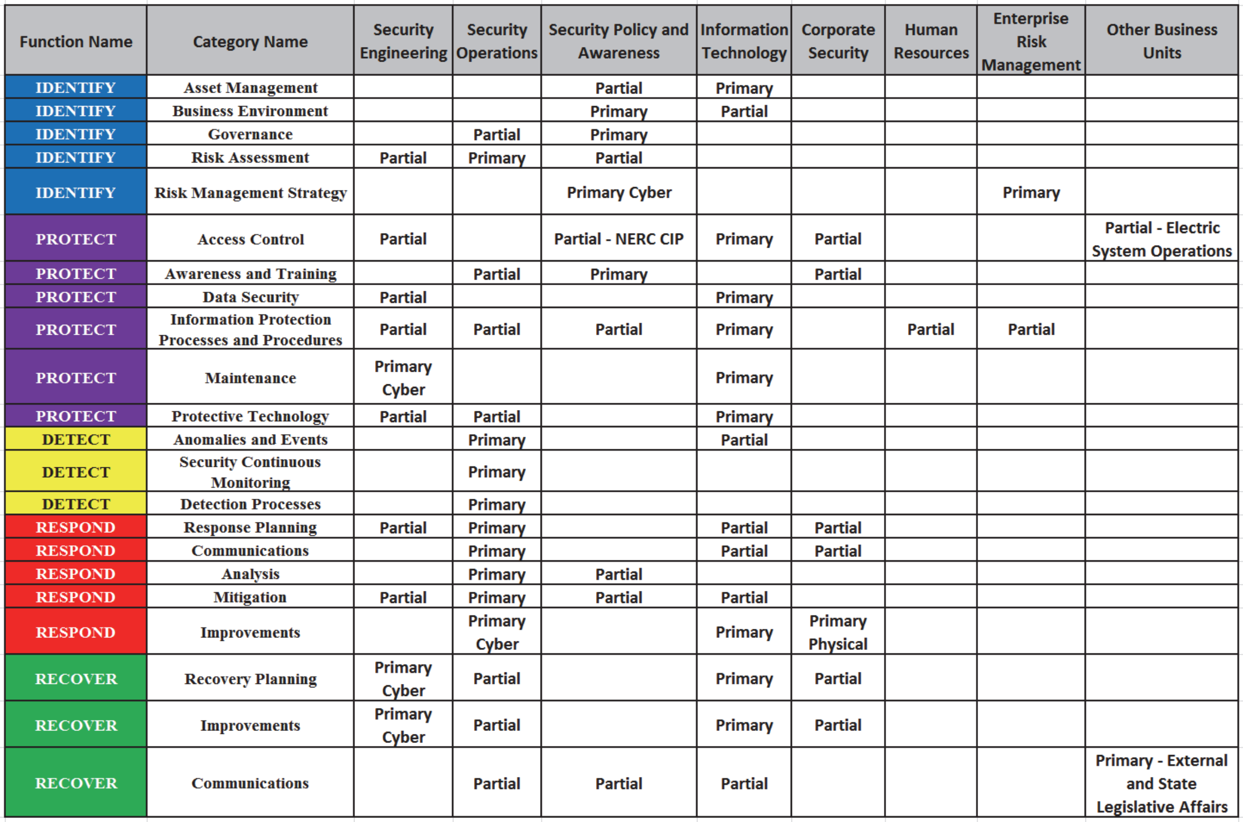
[11] NIST CSF at 9.

Function Name	Category Name	Category Description
PROTECT	Information Protection Processes and Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
PROTECT	Maintenance	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
PROTECT	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT	Anomalies and Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood.
DETECT	Security Continuous Monitoring	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
DETECT	Detection Processes	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND	Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
RESPOND	Communications	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
RESPOND	Analysis	Analysis is conducted to ensure adequate response and support recovery activities.
RESPOND	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
RESPOND	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
RECOVER	Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.
RECOVER	Communications	Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other computer security incident response teams (CSIRTs), and vendors.

The following Table GW-8 describes which organizations support each of the NIST CSF Categories and subcategories. When an organization is responsible for all the subcategories, they are designated as the "Primary." If they are only responsible for some of the subcategories, the designation "Partial" is used. For each of the categories, there is an organization that has primary responsibility.

Table GW-8

NIST CSF Categories and Organizational Responsibilities



Function Name	Category Name	Security Engineering	Security Operations	Security Policy and Awareness	Information Technology	Corporate Security	Human Resources	Enterprise Risk Management	Other Business Units
IDENTIFY	Asset Management			Partial	Primary				
IDENTIFY	Business Environment			Primary	Partial				
IDENTIFY	Governance		Partial	Primary					
IDENTIFY	Risk Assessment	Partial	Primary	Partial					
IDENTIFY	Risk Management Strategy			Primary Cyber				Primary	
PROTECT	Access Control	Partial		Partial - NERC CIP	Primary	Partial			Partial - Electric System Operations
PROTECT	Awareness and Training		Partial	Primary		Partial			
PROTECT	Data Security	Partial			Primary				
PROTECT	Information Protection Processes and Procedures	Partial	Partial	Partial	Primary		Partial	Partial	
PROTECT	Maintenance	Primary Cyber			Primary				
PROTECT	Protective Technology	Partial	Partial		Primary				
DETECT	Anomalies and Events		Primary		Partial				
DETECT	Security Continuous Monitoring		Primary						
DETECT	Detection Processes		Primary						
RESPOND	Response Planning	Partial	Primary		Partial	Partial			
RESPOND	Communications		Primary		Partial	Partial			
RESPOND	Analysis		Primary	Partial					
RESPOND	Mitigation	Partial	Primary	Partial	Partial				
RESPOND	Improvements		Primary Cyber		Primary	Primary Physical			
RECOVER	Recovery Planning	Primary Cyber	Partial		Primary	Partial			
RECOVER	Improvements	Primary Cyber	Partial		Primary	Partial			
RECOVER	Communications		Partial	Partial	Partial				Primary - External and State Legislative Affairs

The NIST CSF Categories supported by the Cybersecurity Department, Security Engineering, Security Operations, Security Policy and Awareness are described in Section IV below.

5. Alternatives Considered

The Companies considered alternatives to the proposed mitigations outlined in the RAMP Report as they developed the proposed mitigation plan for cybersecurity risk. Typically, alternatives analysis occurs when implementing activities, and with vendor selection in order to obtain the best result or product for the cost. The alternatives analysis for the cybersecurity risk plan outlined in the RAMP Report also took into account modifications to the proposed plan and constraints, such as budget and resources.

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 Cybersecurity

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.

The Companies dismissed this alternative in favor of the proposed plan described in the RAMP Report due to resource, financial, and affordability constraints. The RAMP Report 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.

Alternative 2 – Delay Security Capability Implementation

The second alternative that was considered and dismissed in the RAMP Report was to delay security capability implementation in response to a cyber threat, and business and cybersecurity technology changes. If the organization had a higher risk tolerance, then the Cybersecurity 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 cybersecurity 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.

F. Safety Culture

SoCalGas is committed to providing safe and reliable service to its customers. Our safety-first culture focuses on public, customer, and employee safety, with this commitment embedded in every aspect of our work. Our safety culture efforts include developing a trained workforce, operating and maintaining the natural gas infrastructure, and providing safe and reliable natural gas service. The Cybersecurity Program is dedicated to cybersecurity aspects of providing safe and reliable energy delivery while protecting customer information and ensuring compliance with regulations.

Cybersecurity efforts toward achieving a safety culture include the identification of risks, the assignment of specific roles and responsibilities, remediating identified risks and vulnerabilities, tracking cybersecurity threats, providing cybersecurity awareness and training, participating in government, industry, and community information sharing activities, and providing incident response capabilities to mitigate those risks.

The 2015 cybersecurity attack on the Ukrainian Power Grid (UPG) provides insight into how a utility may be impacted by a cyber breach. During that remote cybersecurity attack, power system components were maliciously operated and automation systems were disabled, resulting in disruption of power delivery to customers. A third party gained illegal entry into UPG computers and SCADA systems resulting in multiple substations being remotely controlled and impacted by the malicious actors. UPG's response and recovery activities were 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 eventually recovered by operating in a manual mode.[12] This scenario is just one example of how 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.

Risks associated with unauthorized disclosure of sensitive information continue to increase. Recent examples include the 2015 United States Office of Personnel Management

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

- The 2012 virus attack on Saudi Aramco, which infected 30,000 systems and deleted data from computer hard drives. While the attack did not directly result in an operational impact, this type of incident 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.

(OPM) breach that released sensitive information associated with 21.5 million people[13] and the 2016 Yahoo password breach, which affected 500 million accounts.[14] Most of these events, when applied to the Companies, would have a similar impact in one or more of the risk areas. The Cybersecurity Program applies lessons learned from these and other events, assessments, and exercises to drive cyber safety improvements.

Finally, part of SDG&E's commitment to safety is the continuous implementation of safety training and education of SDG&E's workforce for securely using technology. Well-trained technology users are effective cybersecurity risk mitigations for social engineering attacks such as phishing. The Cybersecurity Program's focus on awareness and outreach is designed to provide safety, security-oriented training, and communication to all Company employees through many activities and programs to improve their cybersecurity behaviors at work and at home. These activities and programs include outreach across the business, providing tools to share information and answer questions, and training in multiple forms, including mandatory cybersecurity training.

G. Cybersecurity Program Summary

As discussed above, the Cybersecurity Program is a cross-cutting business function, which supports key SoCalGas initiatives. The Cybersecurity Department manages cybersecurity risk with strategy, organization, and industry-based best practices.

The current cybersecurity risk mitigation approach 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.

[13] The United States 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 financial, regulatory, legal, and compliance impacts.

[14] 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 financial, regulatory, legal, and compliance 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.

Cybersecurity activities and projects are vital to maintaining the safe, reliable delivery of energy, safeguarding customer information, complying with regulations, and protecting technology assets and information. The following sections provide more detail on activities and projects, describe how they fit into the cybersecurity mitigation control framework, and their costs. Cybersecurity 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.

II. NON-SHARED COSTS

"Non-Shared Services" are activities that are performed by one of the Companies solely for its own benefit. Cybersecurity does not have any non-shared costs.

III. SHARED O&M COSTS

A. Introduction

As described in the testimony of James Vanderhye (Ex. SCG-34/SDG&E-32), shared services are activities performed by a utility shared services department (*i.e.*, functional area) for the benefit of (i) SoCalGas or SDG&E, (ii) Sempra Energy Corporate Center, and/or (iii) any unregulated subsidiaries. The utility providing shared services allocates and bills incurred costs to the entity or entities receiving those services. The primary cost driver for the shared O&M costs is the escalating costs associated with the addition of on-site staff to provide cybersecurity consulting support to other business units during their implementation and development projects to ensure the deployment of secure solutions.

Table GW-9 below summarizes the total shared O&M forecasts for the listed cost categories. The table lists the organization as Access Management. This group has been re-tasked and is more aptly described as Security Engineering - SCG.

TABLE GW-9

Shared O&M Summary of Costs

(In 2016 $) Incurred Costs (100% Level)			
Categories of Management	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
A. ACCESS MANAGEMENT	**238**	**708**	**470**
Total Shared Services (Incurred)	**238**	**708**	**470**

These forecasts are made on a total incurred basis, as well as the shared services allocation percentages related to those costs. Those percentages are presented in my shared services workpapers, along with a description explaining the activities being allocated. The dollar amounts allocated to affiliates are presented in the testimony of James Vanderhye (Ex. SCG-34/SDG&E-32).

The Cybersecurity O&M budget is allocated among the Identify, Protect, Detect, Respond, and Recover cybersecurity risk mitigation Functions, which were described in Section II above.

B. Access Management (Security Engineering-SCG)

TABLE GW-10

Summary of Costs – Security Engineering-SCG

CYBER SECURITY (In 2016 $)			
(In 2016 $) Incurred Costs (100% Level)			
A. ACCESS MANAGEMENT	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. ACCESS MANAGEMENT	238	708	470
Incurred Costs Total	**238**	**708**	**470**

1. Description of Costs and Underlying Activities

The Security Engineering group has three teams: Information Security and Consulting, Production Support, and Security Operations. The group's primary focus is on supporting projects and ensuring the security of applications and the system before the projects are placed in production. In addition, the group regularly implements, administers, and manages cybersecurity technologies. These activities include a combination of labor and non-labor costs.

The Security Engineering group was established within the Cybersecurity Program to provide security architecture, establish security controls (which are combinations of people, process, and/or technology elements that are designed to protect systems and data from harm), support the security operation capability, and consult with the business units on initiatives implementing new technology and business systems to evaluate any risks these new technologies or business systems may pose. The group also oversees the controls necessary to mitigate those potential risks.

The Security Engineering group is responsible for:

- Information Security (IS) Engineering & Consulting – Provides cybersecurity consulting services to SoCalGas, SDG&E, and Corporate Center with the objective of reducing cybersecurity risks associated with projects prior to deployment.
- Production Support – Manages security technologies including firewall rule submission, approval and implementation process, web content filter, SPAM management, and intrusion prevention and detection systems.
- Security Operations – Support enhanced access controls, public key infrastructure, data loss prevention, and endpoint security.

This cost supports the Company's goals of safety and reliability by maintaining and improving the cybersecurity posture by managing cybersecurity risks across the Company. These costs are shared for efficient use of specialized staff and infrastructure. This cost was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-7 by providing Identify, Protect, Respond, and Recover functionality as summarized in Table GW-11 below.

Table GW-11

Summary of Security Engineering Activities

Function	**Category**	**Activities**
Identify	Risk Assessment	Risk Assessment controls support cybersecurity by tracking and communicating cybersecurity risk to the Company's operations, assets, and individuals. The group supports this capability by identifying and tracking potential business impacts and likelihoods of risks found while supporting system development and implementation projects.
Protect	Access Control	The Access Control capability limits access to information and operation systems to authorized users, processes, or devices, and to authorized activities and transactions. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information. The group supports network security and privileged account access controls.
	Data Security	The Data Security capability protects information and data while it is at rest or in transit, which improves cybersecurity by preventing unauthorized viewing, manipulation, or exfiltration of data. The group supports the internal public key infrastructure, data loss prevention controls, and other data protection capabilities.
	Information Protection Processes and Procedures	The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. The group provides support by developing secure baselines, preparing incident responses and recovery procedures for cybersecurity control technology, sharing effectiveness information with appropriate parties, and contributing to continuous improvement processes.
	Maintenance	The Maintenance capability allows prompt maintenance and repair of Company assets in a controlled and timely fashion from either the asset's location or remotely. Many attacks leverage known weaknesses in software. Promptly patching software on assets reduces the likelihood of an impact. The group maintains the cybersecurity control technology they support.
	Protective Technology	Protective Technology capabilities are technical solutions that are managed to ensure the security and resiliency of systems and assets consistently with the related policies, procedures, and agreements. The group supports the protection of networks, reviews audit logs of the systems they support, and assist business implementation projects by implementing logging functions and configuring access controls.

Function	Category	Activities
Respond	Response Planning	Response Planning is the execution of the response plan during or after an event. The group executes their response plan if the systems that they support are affected by an event.
	Mitigation	Mitigation activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. The group supports this capability by tracking risks associated with newly identified vulnerabilities in new systems and those they support.
Recover	Recovery Planning	Recovery Planning is the execution of the recovery plan during or after an event. The group executes their recovery plan if the systems that they support are affected by an event.
	Improvements	The Improvements capability uses lessons learned during recovery planning and processes in future activities. The group reviews and improves their recovery plan for the systems that they support if they are affected by an event.

2. Forecast Methodology

The forecast methodology developed for this cost category is the base year (2016) recorded, plus adjustments. This method is most appropriate because the O&M costs are expected to be consistent with the base year during the GRC period.

3. Cost Drivers

The cost drivers behind this forecast are the continuing need to address increasing exposure to cybersecurity risk to the business and our customers, filling vacant infrastructure technology positions, the utilization of contracted firewall administrative support, and mitigating cybersecurity risk as was described in Section II above and in the RAMP Report. To better support project cybersecurity control implementation, additional staff is being added to be co-located with SoCalGas project teams. These drivers are consistent with California Public Utilities (CPUC) requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

IV. CAPITAL

A. Introduction

Planning for cybersecurity risk mitigation 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. Cybersecurity 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.

Historical activities will continue to be performed. However, due to the evolving nature of the threats associated with this risk, if only the current mitigation activity was to be maintained, the risk would likely grow. Accordingly, the Companies are looking to new capital projects to improve or replace existing security capabilities to address the ever-changing threats and/or supported technologies. While it is possible to plan for technology refresh costs based on the useful lifetime of a solution, it is more difficult to predict reactive technology costs in response to changes in threat capabilities that prematurely make a technology obsolete or require the use of a new technical control.

The Cybersecurity Program continually reassesses planned capital projects to maintain project priorities to balance current project and resource activities based on current cybersecurity risks. A side effect of the risk management adjustments is that project plans are continually reprioritized and restructured. For example, projects defined beyond a 12- to 18-month planning horizon are less likely to be implemented and may be replaced by a higher priority project. Also, projects may happen in different years due to changes in priority and resource availability as a result of the continuous reassessment of threats, known risks, and prioritization.

The capital projects set forth in Table GW-12 below each support different NIST CSF Functions and Categories. Some projects may appear to overlap since a single project does not address all of the sub-capabilities or applicable assets/services, and some projects implement multiple capabilities. The addressed NIST CSF categories are described in more detail for each project below.

Table GW-12

Summary of Capital Projects and Applicable NIST CSF Function/Categories

Function Name	Category Name	Project Name
IDENTIFY	Asset Management	Threat Identification System
IDENTIFY	Business Environment	
IDENTIFY	Governance	
IDENTIFY	Risk Assessment	Enterprise Threat Intelligence Threat Identification System
IDENTIFY	Risk Management Strategy	
PROTECT	Access Control	Critical Gas Infrastructure Protection Firewall Security Information Security Zone Rebuild

Function Name	Category Name	Project Name
		Multi Factor Authentication Refresh My Account Multi Factor Authentication Public Key Infrastructure Rebuild Proof Point Rebuild Wired Network Preventative Controls Converged Perimeter Systems
PROTECT	Awareness and Training	Enterprise Source Code Security
PROTECT	Data Security	CASB (Cloud Data Use) Critical Gas Infrastructure Protection Public Key Infrastructure Rebuild
PROTECT	Information Protection Processes and Procedures	Enterprise Source Code Security Firewall Security Information Security Zone Rebuild Security Orchestration Web Application and Database Firewalls Converged Perimeter Systems
PROTECT	Maintenance	Critical Gas Infrastructure Protection Web Application and Database Firewalls
PROTECT	Protective Technology	Critical Gas Infrastructure Protection Firewall Security Information Security Zone Rebuild Web Application and Database Firewalls Wired Network Preventative Controls Converged Perimeter Systems
DETECT	Anomalies and Events	Critical Gas Infrastructure Protection Security Orchestration Insider Threat Detection / Prevention Network Security Monitoring Perimeter Tap Infrastructure Redesign SCG Network Anomaly Detection Phase 1 Threat Detection Systems
DETECT	Security Continuous Monitoring	Critical Gas Infrastructure Protection Proof Point Rebuild Wired Network Preventative Controls Insider Threat Detection / Prevention SCG Network Anomaly Detection Phase 1 SSL Egress Decryption Threat Detection Systems
DETECT	Detection Processes	Security Orchestration Insider Threat Detection / Prevention Threat Detection Systems
RESPOND	Response Planning	Security Orchestration Threat Response Systems
RESPOND	Communications	Incident Response Secure Collaboration Threat Response Systems
RESPOND	Analysis	Forensics System Rebuild Threat Response Systems
RESPOND	Mitigation	Security Orchestration Threat Response Systems
RESPOND	Improvements	Security Orchestration Threat Response Systems
RECOVER	Recovery Planning	Security Orchestration

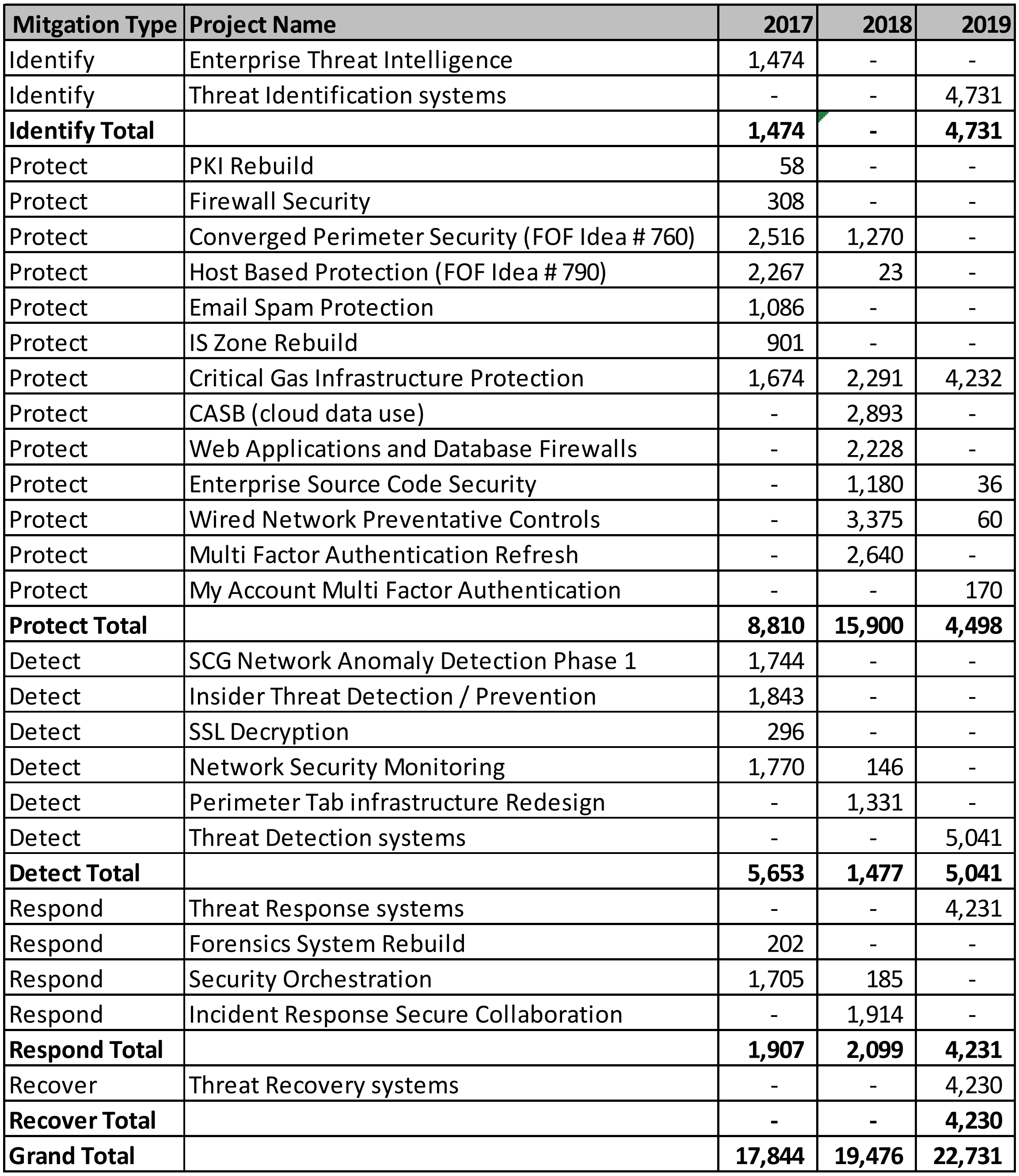
Function Name	Category Name	Project Name
		Threat Recovery Systems
RECOVER	Improvements	Security Orchestration Threat Recovery Systems
RECOVER	Communications	Security Orchestration Threat Recovery Systems

Table GW-13 below summarizes the total capital forecasts for 2017, 2018, and 2019 for the capital projects discussed in the following sections. This table also shows the breakdown of projects by Mitigation Type.[15] Table GW-14 below summarizes the associated total capital forecasts for 2017 and 2018 of the two FOF projects, which I am sponsoring. The two FOF capital projects are discussed in more detail below.

[15] Note the "Overall Summary For Exhibit No. SCG-27-CWP" table on p. 1 of the Capital workpapers shows an incorrect allocation that was not available to update. Refer to Table GW-13 in this testimony for the correct breakdown by mitigation.

TABLE GW-13

Capital Expenditures Summary of Costs
(Thousands of Dollars)



Mitgation Type	Project Name	2017	2018	2019
Identify	Enterprise Threat Intelligence	1,474	-	-
Identify	Threat Identification systems	-	-	4,731
Identify Total		**1,474**	**-**	**4,731**
Protect	PKI Rebuild	58	-	-
Protect	Firewall Security	308	-	-
Protect	Converged Perimeter Security (FOF Idea # 760)	2,516	1,270	-
Protect	Host Based Protection (FOF Idea # 790)	2,267	23	-
Protect	Email Spam Protection	1,086	-	-
Protect	IS Zone Rebuild	901	-	-
Protect	Critical Gas Infrastructure Protection	1,674	2,291	4,232
Protect	CASB (cloud data use)	-	2,893	-
Protect	Web Applications and Database Firewalls	-	2,228	-
Protect	Enterprise Source Code Security	-	1,180	36
Protect	Wired Network Preventative Controls	-	3,375	60
Protect	Multi Factor Authentication Refresh	-	2,640	-
Protect	My Account Multi Factor Authentication	-	-	170
Protect Total		**8,810**	**15,900**	**4,498**
Detect	SCG Network Anomaly Detection Phase 1	1,744	-	-
Detect	Insider Threat Detection / Prevention	1,843	-	-
Detect	SSL Decryption	296	-	-
Detect	Network Security Monitoring	1,770	146	-
Detect	Perimeter Tab infrastructure Redesign	-	1,331	-
Detect	Threat Detection systems	-	-	5,041
Detect Total		**5,653**	**1,477**	**5,041**
Respond	Threat Response systems	-	-	4,231
Respond	Forensics System Rebuild	202	-	-
Respond	Security Orchestration	1,705	185	-
Respond	Incident Response Secure Collaboration	-	1,914	-
Respond Total		**1,907**	**2,099**	**4,231**
Recover	Threat Recovery systems	-	-	4,230
Recover Total		**-**	**-**	**4,230**
Grand Total		**17,844**	**19,476**	**22,731**

TABLE GW-14

Capital Expenditures Summary of SoCalGas Fueling Our Future Costs (Thousands of Dollars)

Project Type	Project Name	2017	2018	2019
FOF	Converged Perimeter Security (FOF Idea # 760)	2,516	1,270	-
FOF	Host Based Protection (FOF Idea # 790)	2,267	23	-
Program Total		**4,783**	**1,293**	**-**

B. Enterprise Threat Intelligence (Identify)

1. Description

The forecast for the Enterprise Threat Intelligence project for 2017 is $1,474,000. SoCalGas plans to build and place this project in service by the test year. This project provides the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. The purpose of this project is to refresh the current solution, expanding it from an electric industry focus to cover all aspects of SoCalGas, SDG&E, and Corporate Center business areas, and to implement the capability to integrate information from an Enterprise Cyber Threat Intelligence resource with other detection and response systems. These projects include purchasing new software, hardware costs, and labor costs to design, implement, integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The specific details regarding the Enterprise Threat Intelligence project are found in my capital workpapers. See Ex. SCG-27-CWP.

The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by implementing security controls to track threat agents, monitor information sources for indications of attack planning, provide vulnerability information relevant to technologies currently in use, and provide indicators of compromise. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Identify capability of Risk Assessment. Risk Assessment controls support cybersecurity by tracking and communicating cybersecurity risk to the Company’s operations, assets, and individuals. This project provides the capability for identifying and documenting threat and vulnerability information from information sharing forums and sources.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to the refresh of technology that is at the end of its life, expanding the capability to address a broader range of threats, and to prepare for future automation for more efficient and quicker utilization of threat intelligence. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

C. Threat Identification Systems (Identify)

1. Description

The forecast for the Threat Identification Systems project for 2019 is $4,731,000. SoCalGas plans to build and place this project in service by the test year. This project will implement multiple capabilities to identify and assess cybersecurity risks. These capabilities are in addition to other threat intelligence and risk assessment capabilities. The capabilities implemented by this effort include some of the technologies developed by the California Energy Systems for the 21st Century (CES-21) Cybersecurity Research & Development (R&D) effort to protect critical infrastructure. Other capabilities implemented by this project will be driven by either emerging threat capabilities or new technology or business functionality leveraged within the critical infrastructure systems and business processes. The specific details regarding the Threat Identification Systems project are found in my capital workpapers. See Ex. SCG-27-CWP.

These projects include purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new systems before putting them into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by improving the cybersecurity posture of critical infrastructure. This project was included in the RAMP Report and supports the NIST CSF capabilities by providing Identify functionality. The Identify Function capabilities addressed by this project include Asset Management and Risk Assessment.

Asset Management controls support cybersecurity by identifying the data, personnel, devices, systems, and facilities that enable the Company's business functions and ensuring they are managed consistently with their relative importance to the business objectives and risk strategy. Risk Assessment controls support cybersecurity by tracking and communicating cybersecurity risk to the Company's operations, assets, and individuals. The project supports this capability by identifying threats to assets used to deliver energy, assessing the risk to the assets, and automatically initiating the mitigation process.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because it includes budgeting estimates based on implementing control capabilities in reaction to future threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes. The forecast has zero-based projects related to the emerging technologies under development by the ratepayer funded CES-21 program.

3. Cost Drivers

The underlying cost drivers for this capital project relate to managing cybersecurity risks to critical infrastructure systems due to evolving threat capabilities and to support the use of new technologies by critical infrastructure systems not addressed elsewhere. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

D. Cloud Access Security Broker Cloud Data Use (Protect)

1. Description

The forecast for the Cloud Access Security Broker (CASB) Cloud Data Use project for 2018 is $2,893,000. SoCalGas plans to build and place this project in service by the test year. CASB provides security monitoring of cloud based services, policy enforcement of sanctioned cloud applications, cloud based data loss prevention (DLP) extensions for Software as a Service (SaaS) applications, and discovery of non-sanctioned cloud service applications. The purpose of this project is to extend data security capabilities found within the internally managed network to cloud SaaS solutions to leverage innovative technologies securely. The specific details regarding the CASB (Cloud Data Use) project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing protective security controls to improve the ability to detect, respond, and recover from a sensitive information extraction and related cybersecurity incident. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect capability of Data Security. The Data Security capability protects information and data while it is at rest or in transit. This capability helps prevent unauthorized viewing or manipulation of data. This project addresses data used with systems outside of the data center.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to supporting and leveraging new technologies. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

E. Critical Gas Infrastructure Protection (Protect)

1. Description

The forecast for the Critical Gas Infrastructure Protection project for 2017, 2018, and 2019 is $1,674,000, $2,291,000, and $4,232,000, respectively. SoCalGas plans to build and place this project in service by the test year. This project will implement multiple capabilities to prevent or detect cybersecurity events to minimize risk likelihood and impacts. These capabilities are in addition to other protection capabilities. The capabilities implemented by this effort include some of the technologies developed by the CES-21 Cybersecurity R&D effort to protect critical infrastructure. Other capabilities implemented by this project will be driven by either emerging threat capabilities or new technology or business functionality leveraged within the critical infrastructure systems and business processes. These projects include purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new systems before putting them into service. The specific details regarding the Critical Gas Infrastructure Protection project are found in my capital workpapers. See Ex. SCG-27-CWP.

The forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining and improving the cybersecurity posture of critical gas infrastructure. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing both Protective and Detective functionality as summarized in Table GW-15 below.

Table GW-15

Summary of Critical Gas Infrastructure Project Activities

Function	**Category**	**Activities**
Protect	Access Control	The Access Control capability limits access to information and operation systems to authorized users, processes, or devices, and to authorized activities and transactions. Access controls improve cybersecurity by preventing unauthorized users from viewing or manipulating systems or information.
	Data Security	The Data Security capability protects information and data while it is at rest or in transit. This capability improves cybersecurity to preventing unauthorized viewing or manipulation of data.
	Maintenance	The Maintenance capability allows prompt maintenance and repair of company assets in a controlled and timely fashion from either the asset's location or remotely. Many attacks leverage known weaknesses in software. Promptly patching software on assets reduces the likelihood of an impact.
	Protective Technology	Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with the related policies, procedures, and agreements. They include protecting communications and control networks, logging, and managing the access authorization process.
Detect	Anomalies and Events	The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions.
	Security Continuous Monitoring	The Security Continuous Monitoring capability is the gathering of information regarding activity and vulnerability status from multiple resources.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because it includes budgeting estimates based on implementing control capabilities in reaction to future threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes. The forecast has zero-based projects related to the emerging technologies under development by the ratepayer funded CES-21 program.

3. Cost Drivers

The underlying cost drivers for this capital project relate to managing cybersecurity risks to critical gas infrastructure systems evolving threat capabilities and to support the use of new technologies by critical infrastructure systems not addressed elsewhere. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

F. Enterprise Source Code Security (Protect)

1. Description

The forecast for the Enterprise Source Code Security project for 2018 and 2019 is $1,180,000 and $36,000, respectively. SoCalGas plans to build and place this project in service by the test year. The Enterprise Source Code Security project provides expanded vulnerability management capabilities with proactive preventative application scanning and static analysis of source code before in-house and/or third-party software is released into production. This project will expand the Company's source code analyzer security scanning system and standardize enhanced procedures for use across software development groups. It will also deploy a centralized repository for dynamic web-based automated security scanning to compliment web-based application security. Firewalls and Intrusion Detection System (IDS) solutions do not provide code level security. The specific details regarding the Enterprise Source Code Security project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing protective security controls to enhance our ability to support cloud-based solutions and by improving the capability to detect security vulnerabilities and exposure prior to production release of code. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect Function capabilities addressed by Awareness and Training and Information Protection Processes and Procedures.

The Awareness and Training capability provides personnel and partners cybersecurity awareness education to adequately train them to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. This project provides secure coding training in addition to the testing tools.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline development practices configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project implements capabilities to support developer-oriented automated and interactive tools, which are integrated with source code control and automate the scanning process so that it becomes an integral part of the system development lifecycle.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to supporting and leveraging new technologies and addressing evolving new threats. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

G. Firewall Security (Protect)

1. Description

The forecast for the Firewall Security project for 2017 is $308,000. SoCalGas plans to build and place this project in service by the test year. This project started in 2016 and implements a firewall rule configuration management tool to maintain consistent configuration, support change management, and provide assessment support of the changes. The specific details regarding the Firewall Security project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing protective security controls to enhance our firewall security management by enforcing consistency and supporting firewall rule changes. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect function capabilities of Access Control, Information Protection Processes and Procedures, and Protective Technology.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Controls improve cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects network integrity, including enforcing network segregation.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project supports change management for firewall rules.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements. This project focuses on protecting communications and control networks.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to supporting and leveraging new technologies and improving the consistency and reducing complexity of firewall architecture. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

H. Information Security Zone Rebuild (Protect)

1. Description

The forecast for the Information Security (IS) Zone Rebuild project for 2017 is $901,000. SoCalGas plans to build and place this project in service by the test year. This project is a refresh of the server hardware, networking infrastructure, and rack infrastructure supporting the technology operated and maintained by the Cybersecurity Department to support cybersecurity control solutions. The specific details regarding the IS Zone Rebuild project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and migrate systems to the new solution, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability, and refreshing infrastructure hardware that is no longer supported to maintain a reliable and available cybersecurity infrastructure for cybersecurity supported systems. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect function capabilities of Access Control, Information Protection Processes and Procedures, and Protective Technology.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects network integrity, including enforcing network segregation and managing access to cybersecurity assets.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project supports maintaining a secure configuration baseline.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with related policies, procedures, and agreements. This project focuses on controlling access and protecting communications and control networks.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to refresh aging hardware infrastructure, which is no longer supported by the vendor, before equipment failure. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by improving the reliability of the cybersecurity control infrastructure. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

I. Multi Factor Authentication Refresh (Protect)

1. Description

The forecast for the Multi Factor Authentication Refresh project for 2018 is $2,640,000. SoCalGas plans to build and place this project in service by the test year. This project is a refresh, extension, and enhancement of the multi-factor authentication capability used to increase confidence in a user's authentication credentials. Multi-factor authentication will be used by all users and vendors when accessing systems or information with privileged access, remote access, or when using third party systems, such as cloud services. The specific details regarding the Multi Factor Authentication Refresh project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by improving user authentication for privileged access, remote access, or when using third party systems, such as cloud services, with company information. This project was included in the RAMP Report and supports the NIST

CSF capabilities specified in Table GW-12 by providing the Protect Function capability Access Control.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects assets and information by increasing user identity authentication requirements when there is a greater exposure to risk of an unauthorized user.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project are to refresh the existing multi-factor authentication infrastructure, extend the capability to all users and vendors, and provide support for third-party systems hosting Company information and services, such as cloud service, to enable the use of innovative new technologies. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by providing a capability to increase the confidence that the user is who they claim to be when accessing assets considered to be at a higher risk. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

J. My Account Multi Factor Authentication (Protect)

1. Description

The forecast for the My Account Multi Factor Authentication project for 2019 is $479,000. SoCalGas plans to initiate and pilot this project starting in the test year. This project implements several multi-factor authentication capability options for customers using the My Account portal to protect customer information. The specific details regarding the My Account Multi Factor Authentication project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by enhancing customer authentication for My Account in order to better protect their personal and energy information. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect Function capability Access Control.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects assets and information by increasing customer identity authentication requirements to reduce the risk of exposure of their information to an unauthorized user.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to implement multi-factor authentication options for customers to access their information via the My Account portals. The capability implements cybersecurity controls to address evolving threat capabilities. Multi-factor authentication reduces the likelihood of unauthorized activity and access, the resulting impact to safety and reliability, and customer privacy impacts. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

K. Public Key Infrastructure Rebuild (Protect)

1. Description

The forecast for the Public Key Infrastructure Rebuild project for 2017 is $58,000. SoCalGas plans to build and place this project in service by the test year. This project started in 2015 and is a refresh of the Public Key Infrastructure (PKI) to update obsolete cryptography. PKI technology is used to identify devices and applications, protect data in-transit, and to verify the integrity of software. The specific details regarding the Public Key Infrastructure Rebuild project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, to test the functionality of the new system before putting it into service, and migrate devices and applications to the new infrastructure. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by refreshing protective security controls and industry guidelines for best practices. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect function capabilities of Access Control and Data Security.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project provides verifiable device authentication. The Data Security capability protects information and data while it is at rest or in transit. This capability improves cybersecurity by preventing unauthorized viewing or manipulation of data while it is in transit and by providing a mechanism to verify software has not been modified by an unauthorized agent.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is the need to replace obsolete cybersecurity controls. In this case, the supported encryption algorithms had been deprecated. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

L. E-Mail Spam Protection (Protect)

1. Description

The forecast for the Email Spam Protection project for 2017 is $1,086,000. SoCalGas plans to build and place this project in service by the test year. This project is a refresh of the system used to identify and block email spam, phishing, and malware defense for all internal and external email. The specific details regarding the Email Spam Protection project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project supports the Company's goals for safety and reliability by refreshing protective controls to block unauthorized or undesirable use of email to trick users or deliver malware. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect function capability Access Control and the Detect function of Security Continuous Monitoring.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects against unauthorized use of company resources.

The Security Continuous Monitoring capability is the gathering of information regarding activity and vulnerability status from multiple resources. This project implements a capability to identify and block malicious software and mobile code, as well as email social engineering attacks on users.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is the need to refresh existing technology in order to maintain current protections versus malware and phishing attacks before the information reaches the user. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

M. Security Orchestration (Respond)

1. Description

The forecast for the Security Orchestration project for 2017 and 2018 is $1,705,000 and $185,000, respectively. SoCalGas plans to build and place this project in service by the test year.

This project implements a security orchestration infrastructure that automates repeatable Information Security Operations Center tasks to respond more quickly and to allow analysts to focus on higher value tasks. The specific details regarding the Security Orchestration project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by improving response times to incidents, allowing better resource allocation to identify and prevent other threats, and supporting continuous process improvement. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing Protect, Detect, Respond, and Recover function capabilities as summarized in Table GW-16 below.

Table GW-16

Summary of Security Orchestration Project Activities

Function	**Category**	**Activities**
Protect	Information Protection Processes and Procedures	This capability addresses adherence to policies and procedures to manage the protection of assets. This project supports this capability by implementing and supporting incident response and recovery plans.
Detect	Anomalies and Events	The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. This project supports this capability by implementing incident alert thresholds and performing an initial analysis of the impact of the events within predetermined guidelines.
	Detection Process	Detection Processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. This project supports this capability by automatically communicating and providing a framework for continuous improvement.
Respond	Resource Planning	Response Planning is the execution of the response plan during or after an event.
	Improvements	The Improvements capability improves organizational response activities by incorporating lessons learned from current and previous detection/response activities. This project supports these capabilities by implementing and supporting incident response plans and providing a framework their continuous improvements.

Function	Category	Activities
Recover	Recovery Planning	Recovery Planning is the execution of the recovery plan during or after an event.
	Improvements	The Improvements capability uses lessons learned during recovery planning and processes in future activities. This project supports these capabilities by implementing and supporting incident recovery plans and providing a framework their continuous improvements.
	Communications	Communications during recovery involve the coordination of multiple stakeholders that may be impacted. The group supports the capability via communications with internal stakeholders and executive and management teams. This project can automate key communications and notifications.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to more efficiently use resources by implementing a framework for continuous improvements to address evolving threat capabilities. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

N. Web Application and Database Firewalls (Protect)

1. Description

The forecast for the Web Application and Database Firewalls project for 2018 is $2,228,000. SoCalGas plans to build and place this project in service by the test year. This project implements a technology to provide an added layer of protection to alert and block attacks targeting web applications, their databases, and the supporting application components and libraries. The specific details regarding the Web Application and Database Firewalls project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing protective security controls to enhance our firewall security management by enforcing consistency and supporting firewall rule changes. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect Function capabilities: Information Protection Processes and Procedures, Maintenance, and Protective Technology.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project supports web application and database vulnerability mitigation when those vulnerabilities are not known or discovered prior to going into production.

The Maintenance capability allows prompt maintenance and repair of company assets in a controlled and timely fashion from either the asset's location or remotely. Many attacks leverage known weaknesses in software. Promptly patching software on web applications may not always be feasible. This technology provides compensating mitigation during the period between when a vulnerability is discovered and when it can be mitigated.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with related policies, procedures, and agreements. This project focuses on protecting web applications and databases.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to provide additional risk mitigation for addressing internet-based attacks targeting web applications and databases using evolving threat capabilities. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by implementing a mechanism to disrupt attacks quickly while a long-term mitigation is implemented. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

O. Wired Network Preventative Controls (Protect)

1. Description

The forecast for the Wired Network Preventative Controls project for 2018 and 2019 is $3,375,000 and $60,000, respectively. SoCalGas plans to build and place this project in service by the test year. This project implements protective controls to manage authorized and unauthorized device access to wired networks at all facilities and field sites providing wired, transmission control protocol (TCP)/internet protocol (IP) connectivity. The solution will provide a mechanism to enforce connection policies and to quarantine and alert when suspect devices attempt to connect to the network. The specific details regarding the Wired Network Preventative Controls project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing protective security controls to protect communications, data, and control networks as well as preserve network integrity. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect Function capabilities of Access Control, Information Protection Processes and Procedures, and Protective Technology. The project also supports the Detect function capability Security Continuous Monitoring.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects network integrity including enforcing network integrity.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with related policies, procedures, and agreements. This project focuses on protecting communications and control networks by managing access of authorized devices and unauthorized devices based on policies.

The Security Continuous Monitoring capability is the gathering of information of activity and vulnerability status from multiple resources. This project supports this capability by monitoring for unauthorized devices.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to provide additional risk mitigation for managing device access to wired networks, both Corporate network and control network connections. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

P. Insider Threat Detection / Prevention (Detect)

1. Description

The forecast for the Insider Threat Detection / Prevention project for 2017 is $1,843,000. SoCalGas plans to build and place this project in service by the test year. This project deploys new user behavior and network activity anomaly detection technologies as well as enhancements of existing security technologies already in production on the corporate network to identify possible cyber insider threat activities. The specific details regarding the Insider Threat Detection / Prevention project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by implementing detective security controls to identify unauthorized or irregular insider technology usage. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Detect Function capabilities of Anomalies and Events, Detection Processes, and Security Continuous Monitoring.

The Anomalies and Events capability analyzes collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. This project focuses on anomalous insider activities. Detection Processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. The project extends current processes and procedures to identify insider threat activities. The

Security Continuous Monitoring capability is the gathering of information of activity and vulnerability status from multiple resources. This project supports the establishment of normal activity baseline, which is used to determine suspicious deviations from normal activity.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to provide additional risk mitigation for insider based threats by enhancing detective capabilities. This threat is magnified by increased threat agent aggression and resources as well as incorporating new technology to enable a mobile workforce. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

Q. Network Security Monitoring (Detect)

1. Description

The forecast for the Network Security Monitoring project for 2017 and 2018 are $1,770,000 and $146,000, respectively. SoCalGas plans to build and place this project in service by the test year. This project implements a consolidated network security monitoring capability including packet capture at the network perimeter. This project will evaluate and deploy technologies to consolidate network security monitoring from existing network security tools, and will add new capabilities to support the analysis of flow data, packet meta data, and full packet data at key network transit points. The specific details regarding the Network Security Monitoring project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing detective security controls to analyze traffic from multiple sources, including deeper into the communication packets, to identify potential threats and indicators of compromise. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the

Detect Function capability, Anomalies and Events. The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. This project enables a more consolidated, deeper inspection into collected data.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to provide additional risk mitigation for addressing network based attacks using evolving threat capabilities. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by implementing a mechanism to disrupt attacks quickly while a long-term mitigation is implemented. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

R. Perimeter Tap Infrastructure Redesign (Detect)

1. Description

The forecast for the Perimeter Tap Infrastructure Redesign project for 2018 is $1,331,000. SoCalGas plans to build and place this project in service by the test year. This project implements a network device in the network perimeter to support cybersecurity and network monitoring tools connections. The specific details regarding the Perimeter Tap Infrastructure Redesign project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by integrating network devices at key locations of the network to allow rapid troubleshooting in support of cybersecurity monitoring and network monitoring. This solution enables other monitoring and analysis detection capabilities. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Detect Function capability of Anomalies and Events. The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. This project enables a monitoring equipment to be quickly moved between pre-identified locations in the perimeter.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to pre-position monitoring taps within the perimeter to support rapid redeployment of tools without network interruptions in response to new types of threats, among other things. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by supporting a more responsive and adaptive detection capability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

S. SCG Network Anomaly Detection Phase 1 (Detect)

1. Description

The forecast for the SCG Network Anomaly Detection Phase 1 project for 2017 is $1,744,000. SoCalGas plans to build and place this project in service by the test year. This project will deploy industrial control systems (ICS)/SCADA network anomaly detection devices. Deployment of these devices will focus on key gas control transmission locations and compressor stations. The project will integrate this new technology into SoCalGas logging infrastructure and security incident and event monitoring solutions so events and alerts can be viewed and responded to by Security Operations Center (SOC). The specific details regarding the SCG Network Anomaly Detection Phase 1 project are found in my capital workpapers. See Ex. SCG-27-CWP.

The project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality and compliance of the new system before putting it into service. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by providing visibility into ICS/SCADA network traffic. This project was included in the RAMP Report as RAMP-Post

Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing Detect Function capabilities.

The Detect function capabilities addressed by this project include Anomalies and Events and Security Continuous Monitoring. The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. The Security Continuous Monitoring capability is the gathering of information of activity and vulnerability status from multiple resources.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to deploy control network monitoring devices into the gas infrastructure to detect and alert on anomalous network activity. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by enhancing visibility into the control network activity. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

T. SSL Decryption (Detect)

1. Description

The forecast for the SSL Decryption project for 2017 is $296,000. SoCalGas plans to build and place this project in service by the test year. This project will implement technology to improve the inspection of network data. The technology will be implemented at the perimeters in both data centers. Traffic will be inspected by multiple IS tools, intrusion prevention system (IPS), malware detection, antivirus, data loss prevention and passive vulnerability detection to ensure full inspection. The specific details regarding the secure sockets layer (SSL) Decryption project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by enhancing visibility into network traffic for comprehensive monitoring. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Detect Function capability, Security Continuous Monitoring. The Security Continuous Monitoring capability is the gathering of information of activity and vulnerability status from multiple resources.

2. Forecast Method

The forecast method developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to enhance detection capabilities to help address evolving threat capabilities that utilize SSL encryption. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by supporting a more responsive and adaptive detection capability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

U. Threat Detection Systems (Detect)

1. Description

The forecast for the Threat Detection Systems project for 2019 is $4,732,000.   SoCalGas plans to build and place this project in service by the test year. This project will implement multiple capabilities to detect cybersecurity risks. These capabilities are in addition to other detection system capabilities. The capabilities implemented by this effort include some of the technologies developed by the CES-21 Cybersecurity R&D effort to protect critical infrastructure. Other capabilities implemented by this project will be driven by either emerging threat capabilities or new technology or business functionality leveraged within the critical infrastructure systems and business processes. The specific details regarding the Threat Detection Systems project are found in my capital workpapers. See Ex. SCG-27-CWP.

These projects include purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting them into service. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by improving the cybersecurity posture of critical infrastructure. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing Detect functionality. The

Detect Function capabilities addressed by this project include Anomalies and Events, Detection Processes, and Security Continuous Monitoring.

The Anomalies and Events capability analyzes the collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. Detection Processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. The Security Continuous Monitoring capability is the gathering of information of activity and vulnerability status from multiple resources. This project addresses all three of these capabilities by leveraging multiple sources of information to improve identification of anomalous activity.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because it includes budgeting estimates based on implementing control capabilities in reaction to future threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes. The forecast has zero-based projects related to the emerging technologies under development by the ratepayer funded CES-21 program.

3. Cost Drivers

The underlying cost drivers for this capital project relate to managing cybersecurity risks to critical infrastructure systems from evolving threat capabilities and to support the use of new technologies by critical infrastructure systems not addressed elsewhere. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

V. Forensics System Rebuild (Respond)

1. Description

The forecast for the Forensics System Rebuild project for 2017 is $202,000. SoCalGas plans to build and place this project in service by the test year. This project started in 2016 and is a refresh of the Company’s forensics infrastructure. The specific details regarding the Forensics System Rebuild project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems, to test the functionality of the new system before putting it into service, and to migrate devices and applications to the new infrastructure. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by refreshing the forensics technology to maintain industry best practices. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-12 by providing the Response function capability Analysis. The Analysis capability is conducted to ensure adequate response and recovery activities. This project refreshes the cyber forensics services infrastructure.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to refresh the technology supporting the forensics business processes. The capability implements cybersecurity controls that maintain current forensics capability to capture and analyze incident information. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

W. Incident Response Secure Collaboration (Respond)

1. Description

The forecast for the Incident Response Secure Collaboration project for 2018 is $1,914,000. SoCalGas plans to build and place this project in service by the test year. This project will deploy a scalable communication and coordination platform that can be used during large cybersecurity incidents to coordinate incident response activities across a potentially large internal audience of cybersecurity, information technology, and business stakeholder groups. This project will investigate and deploy a communication and coordination platform that can be securely leveraged on the corporate network, and off the corporate network when there are major availability issues. The specific details regarding the Incident Response Secure Collaboration project are found in my capital workpapers. See Ex. SCG-27-CWP.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company’s goals for safety and reliability by deploying a secure collaboration capability to support secure communications during a cybersecurity incident response. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Response function capability Communications. The Communications capability ensures response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. This project implements a secure communication which is not reliant on corporate networks if they are unavailable.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is to enhance detection capabilities to address evolving threat capabilities. The capability implements cybersecurity controls that reduce the likelihood of unauthorized activity and the resulting impact to safety and reliability by supporting a more responsive and adaptive detection capability. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

X. Threat Response Systems (Respond)

1. Description

The forecast for the Threat Response Systems project for 2019 is $4,231,000. SoCalGas plans to build and place this project in service by the test year. This project will implement multiple capabilities to respond to cybersecurity risks. These capabilities are in addition to other response system capabilities. The capabilities implemented by this effort include some of the technologies developed by the CES-21 Cybersecurity R&D effort to protect critical infrastructure. Other capabilities implemented by this project will be driven by either emerging threat capabilities or new technology or business functionality leveraged within the critical infrastructure systems and business processes. The specific details regarding the Threat Response Systems project are found in my capital workpapers. See Ex. SCG-27-CWP.

These projects include purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting them into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by improving the cybersecurity response capability of critical infrastructure. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing Respond functionality. The Respond function capabilities addressed by this group include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Response Planning is the execution of the response plan during or after an event. The Communications capability ensures response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. The Analysis capability is conducted to ensure adequate response and recovery activities. The group provides cyber forensics services in support of this capability. Mitigation activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. The Improvements capability improves organizational response activities by incorporating lessons learned from current and previous detection/response activities.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because it includes budgeting estimates based on implementing control capabilities in reaction to future threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes. The forecast has zero-based projects related to the emerging technologies under development by the ratepayer funded CES-21 program.

3. Cost Drivers

The underlying cost drivers for this capital project relate to managing cybersecurity risks to critical infrastructure systems from evolving threat capabilities and to supporting the use of new technologies for threat response by critical infrastructure systems not addressed elsewhere. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

Y. Threat Recovery Systems (Recover)

1. Description

The forecast for the Threat Recovery Systems project for 2019 is $4,230,000. SoCalGas plans to build and place this project in service by the test year. This project will implement multiple capabilities to recover from threats. These capabilities are in addition to other system recovery capabilities. The capabilities implemented by this project are driven by emerging threat capabilities, new technology, or business functionality leveraged within the critical infrastructure systems and business processes or as the result of assessments, exercises, or incidents.

As more of the server infrastructure is consolidated, cybersecurity systems that are integral to recovering from an incident need to be redesigned to have high availability. For example, this project includes deploying new infrastructure for the Privileged Access system and the PKI system. The Privileged Access system is used to manage system administrator accounts and sessions. The PKI system is used to identify devices, such as servers and workstations, secure communications, and sign software. Additional efforts would be added to this project as a result of improvements identified after exercises, tests, or incidents. The specific details regarding the Threat Recovery Systems project are found in my capital workpapers. See Ex. SCG-27-CWP.

These projects include purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting them into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by improving the recovery capability needed to return to a trustworthy operational state after an incident. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing Recovery functionality. The Recovery Function capabilities addressed by this project include Recovery Planning, Improvements, and Communications.

Recovery Planning is the execution of the recovery plan during or after an event. The group supports recovery plan if the systems that they support are affected by an event. The Improvements capability uses lessons learned during recovery planning and processes in future activities. The group reviews and improves their recovery plan for the systems that they support if they affected by an event. Communications during recovery involve the coordination of multiple stakeholders that may be impacted. The group supports the capability via communications with internal stakeholders and executive and management teams.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because it includes budgeting estimates based on implementing control capabilities in reaction to future threats due to hostile agents and increasing attack surfaces due to the application of new technology, increasing integration with third parties, and changing business processes. The forecast has zero-based projects related to the emerging technologies under development by the ratepayer funded CES-21 program.

3. Cost Drivers

The underlying cost drivers for this capital project relate to managing cybersecurity risks to critical infrastructure systems evolving threat capabilities and to support the use of new recovery technologies by critical infrastructure systems not addressed elsewhere. Documentation of these cost drivers is included in my capital workpapers. See Ex. SCG-27-CWP.

Z. Converged Perimeter Systems (Protect)

1. Description

The forecast for the Converged Perimeter Systems project for 2017 and 2018 are $2,516,000 and $1,270,000 respectively. SoCalGas plans to build and place this project in service by the test year. This project will utilize a converged security control model to facilitate network boundary level protection for the Company's computing systems and data. This approach will utilize a single piece of network security infrastructure to consolidate multiple cybersecurity functions. The concept is to combine the existing components into a common device and upgrade the existing infrastructure.

The scope of this project will focus on firewalls (4) and intrusion prevention devices (6) at the data center perimeters. The specific details regarding the Converged Perimeter Systems project are found in my capital workpapers. See Ex. SCG-27-CWP. This project is also a Fueling Our Future project.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by reducing the complexity of the network perimeter. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing the Protect Function capabilities of Access Control, Information Protection Processes and Procedures, and Protective Technology.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Control improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects network integrity including enforcing perimeter controls combining firewall and intrusion detection/prevention system controls.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project enforces network traffic policies at the perimeter.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with the related policies, procedures, and agreements. This project protects networks and devices within the perimeter.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project relate to the consolidation of perimeter network protections into a single platform to gain the advantages of new cybersecurity technologies. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

AA. Host Based Protection (Protect)

1. Description

The forecast for the Host Based Protection project for 2017 and 2018 is $2,267,000 and $23,000, respectively. SoCalGas plans to build and place this project in service by the test year. This project would investigate and implement an endpoint security solution that would allow an endpoint to be protected in a hostile environment. Both servers and workstations would be included in the scope of this project so that endpoints will be better protected and resilient when located outside the protected perimeter, such as being placed in cloud environments or connecting to the network while working offsite. The specific details regarding the Host Based Protection project are found in my capital workpapers. See Ex. SCG-27-CWP. This project is also a Fueling Our Future project.

This project includes purchasing new software, hardware costs, and labor costs to design, implement, and integrate the solution with related systems and to test the functionality of the new system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing cybersecurity protections on servers and workstations to provide defense in depth while within the protected perimeter and maintain a secure posture when logically or physically outside the perimeter. This project was included in the RAMP Report and supports the NIST CSF capabilities specified in Table GW-12 by providing Protect function capabilities: Access Control, Information Protection Processes and Procedures, and Protective Technology.

The Access Control capability supports the authorization credentials and limits access to information and operation systems to authorized users. Access Controls improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information and validating the access of authorized users. This project protects network integrity including enforcing perimeter type controls such as firewall and intrusion detection/prevention systems on the host.

The Information Protection Processes and Procedures capability addresses adherence to policies and procedures to manage the protection of assets. Secure baseline configurations should be developed early in the system development lifecycle and then updated via change management procedures to support continuous improvements. This project enforces network traffic policies at the host.

Protective Technology capabilities are technical solutions that are managed to ensure the security and resilience of systems and assets consistently with the related policies, procedures, and agreements. This project protects networks and devices within or outside of the perimeter.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because cost estimates are specific to the project and assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is supporting new technologies by integrating network protections into each platform to reduce risks associated with locating servers and workstation outside of the protected perimeter. Documentation of this cost driver is included in my capital workpapers. See Ex. SCG-27-CWP.

V. CONCLUSION

These forecasts are expected to allow SoCalGas to continue to maintain the current security posture in an environment of evolving threat agent capabilities and increasing adoption of innovative technology.

This concludes my prepared direct testimony.

VI. WITNESS QUALIFICATIONS

My name is Gavin Worden. My primary work location is 10975 Technology Place, San Diego, CA 92127-1811. I am currently employed by SDG&E as the Director of the IT Operations department for Corporate Center, SoCalGas, and SDG&E.   In this role, I oversee the Cybersecurity Operations for Corporate Center, SoCalGas, and SDG&E.

Previously my positions have included Information Security Manager at Sempra Energy and at the IT Division of SDG&E as the Information Security Operations Center Manager. Prior to that I was the Assistant Deputy Director for the San Diego Law Enforcement Coordination Center, where I provided cybersecurity and intelligence support to both government and private sector organizations.

I am a *cum laude* graduate of San Diego State University, where I received a Bachelor of Science in Business Administration. I also earned a Master of Business Administration degree from the University of San Diego. My professional certifications include International Information Systems Security Certification Consortium (ISC2) Certified Information Systems Security Professional (CISSP), International Council of E-Commerce Consultants (EC-Council) Certified Ethical Hacker (CEH), and Information Assurance Certification Review Board (IACRB) Certified Penetration Tester (CPT).

I have not previously testified before the Commission.

APPENDIX A – GLOSSARY OF TERMS

CASB: Cloud Access Security Broker

CES-21: California Energy Systems for the 21st Century

CPUC: California Public Utilities Commission

CIP: Critical Infrastructure Protection

CSF: Cybersecurity Framework

CSIRT: Computer Security Incident Response Team

DDoS: Distributed Denial of Service

DLP: Data Loss Prevention

FERC: Federal Energy Regulatory Commission

FOF: Fueling Our Future

GRC: General Rate Case

IP: Internet Protocol

ICS: Industrial Control System

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IS: Information Security

ISOC: Information Security Operations Center

IT: Information Technology

NERC: North American Electric Reliability Corporation

NIST: National Institute of Standards and Technology

O&M: Operations and Maintenance

PKI: Public Key Infrastructure

R&D: Research and Development

RAMP: Risk Assessment Mitigation Phase

SaaS: Software as a Service

SCADA: Supervisory Control and Data Acquisition

SDG&E: San Diego Gas & Electric Company

SOC: Security Operations Center

SoCalGas: Southern California Gas Company

SSL: Secure Sockets Layer

TCP/IP: Transmission Control Protocol/Internet Protocol

TY: Test Year

UPG: Ukrainian Power Grid

SCG 2019 GRC Testimony Revision Log – December 2017

Exhibit	Witness	Page	Line	Revision Detail
SCG-27	Gavin Worden	GW-3, GW-5	TABLE GW-2A, TABLE GW-5A	Changed “TY 2019 Estimated Incremental (000s)” from 708 to 470. Changed “Total (000s)” from 470 to 708.
SCG-27	Gavin Worden	GW-28 – GW-29	2-3	Added sentence: “This table also shows the breakdown of projects by Mitigation Type.” And inserted an associated Footnote 15. Deleted extra table below Table GW-13.