Company: San Diego Gas & Electric Company (U 902 M)
Proceeding: 2019 General Rate Case
Application: A.17-10-___
Exhibit: SDG&E-25

SDG&E

DIRECT TESTIMONY OF GAVIN WORDEN

(CYBERSECURITY)

October 6, 2017

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

Doc #317158

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)	6,567	7,907	1,340
Total O&M	**6,567**	**7,907**	**1,340**

CYBERSECURITY (In 2016 $)				
	2016 Adjusted-Recorded (000s)	Estimated 2017 (000s)	Estimated 2018 (000s)	Estimated 2019 (000s)
Total CAPITAL	**0**	**6,146**	**7,232**	**5,618**

Summary of Requests

- Provide cybersecurity support services that directly contribute to San Diego Gas & Electric Company's (SDG&E) 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.

SDG&E 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 SDG&E. 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)	6,567	7,907	1,340
Total O&M	**6,567**	**7,907**	**1,340**

CYBERSECURITY (In 2016 $)				
	2016 Adjusted-Recorded (000s)	Estimated 2017 (000s)	Estimated 2018 (000s)	Estimated 2019 (000s)
Total CAPITAL	**0**	**6,146**	**7,232**	**5,618**

The Cybersecurity Department (formerly the Information Security Department) is responsible for cybersecurity risk management of the information and operational technologies for SDG&E, Southern California Gas Company (SoCalGas), and Sempra Energy Corporate Center (Corporate Center). Cybersecurity risk management is performed through various activities 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 SDG&E, SoCalGas, 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 information technology (IT) groups so that they can perform their functions safely, reliably, and securely.

My testimony describes 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 SDG&E, SoCalGas, 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.) SDG&E-24). The cybersecurity risk management activities set forth in my testimony correspondingly benefit SDG&E, SoCalGas, and Corporate Center. The primary cost drivers for the cybersecurity costs discussed below are 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 framework, NIST CSF, functional areas.

In addition to sponsoring my own organization's costs, my testimony also supports the costs associated with a group of capital projects focused on improving the cybersecurity of SDG&E's electric distribution system (Grid Modernization Projects), which are discussed in the testimony of Alan Colton (Ex. SDG&E-14).

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.

While preparing my GRC forecasts, I continued to evaluate the scope, schedule, resource requirements, synergies of RAMP-related projects and programs, and alternative mitigations.

[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).

Therefore, the final representation of RAMP costs provided herein may differ from the ranges shown in the original RAMP Report. Tables GW-2A and GW-2B below 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)**
SDG&E-7 Cyber Security	4,198	3,740	7,938
Total O&M	**4,198**	**3,740**	**7,938**

TABLE GW-2B

Summary of RAMP Capital-Related Costs

CYBERSECURITY (In 2016 $)			
Categories of Management	**Estimated 2017 (000s)**	**Estimated 2018 (000s)**	**Estimated 2019 (000s)**
A. Detect	110	0	0
B. Identify	876	0	0
C. Protect	2,496	3,174	3,686
D. Grid Modernization	2,664	4,058	1,932
Total	**6,146**	**7,232**	**5,618**

C. Organization of Testimony

My testimony is organized as follows:

- Section II provides a summary of SDG&E and SoCalGas' RAMP, defines cybersecurity risk, provides background on the Cybersecurity Program, discusses the Company's cybersecurity strategy and risk management process, and sets forth SDG&E's safety culture.
- Section III states that SDG&E has no 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.

II. RISK ASSESSMENT MITIGATION PHASE AND SAFETY CULTURE

A. Risk Assessment Mitigation Phase

Certain costs sponsored by my testimony are linked to mitigating cybersecurity, which is a top safety risk that was identified in the RAMP Report and is further described in Table GW-3:

TABLE GW-3

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 discussion, 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 Table GW-4 below. RAMP-related costs are further described in Sections III, IV, and V below as well as in my workpapers.

TABLE GW-4

RAMP Risks Associated with this Testimony

CYBERSECURITY (In 2016 $)			
RAMP Report Risk Chapter	**2016 Embedded Base Costs (000s)**	**TY 2019 Estimated Incremental (000s)**	**Total (000s)**
SDG&E-7 Cyber Security	4,198	3,740	7,938
Total O&M	**4,198**	**3,740**	**7,938**

CYBERSECURITY (In 2016 $)				
RAMP Report Risk Chapter	**2016 Embedded Base Costs (000s)**	**Estimated 2017 (000s)**	**Estimated 2018 (000s)**	**Estimated 2019 (000s)**
SDG&E-7 Cyber Security	0	6,146	7,232	5,618
Total Capital	**0**	**6,146**	**7,232**	**5,618**

While the starting point for consideration of the risk mitigation effort and cost was the RAMP Report, SDG&E's 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.

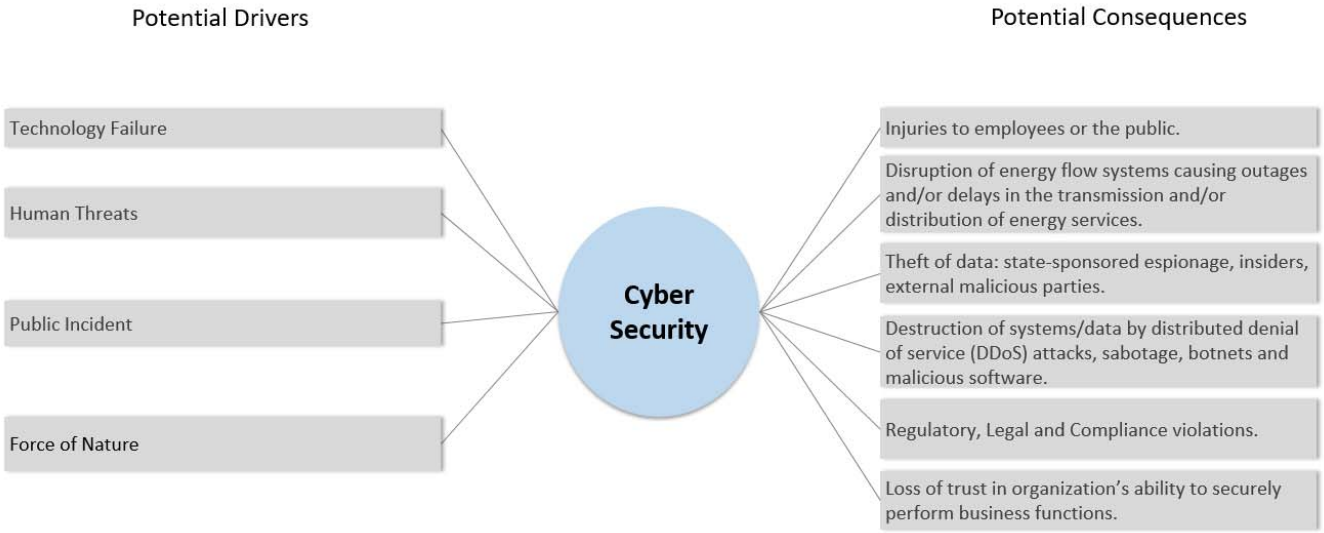
Electric and gas operations, safety systems, information processing, and other utility functions are increasingly reliant on technology, automation, and integration with other systems.

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



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 described in Table GW-5 below.

Table GW-5

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.

- 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 SDG&E, SoCalGas, 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 cybersecurity 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 utilizing 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 multiple sources of information and assessments of risk mitigation practices and critical

[4] In Application (A.) 15-05-002, SDG&E's Safety Model Assessment Proceeding (S-MAP), SDG&E provided the supporting testimony of Scott King, which described the Cybersecurity Program and the cybersecurity risk management process.

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 Companies 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 Framework 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 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]

---

[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).

[6] NIST CSF at 8-9.

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 Framework. 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 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

[7] NIST CSF at 8.
[8] NIST CSF at 8.

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.

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

[9] NIST CSF at 8.
[10] NIST CSF at 8-9.

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 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 core five Functions are described in Table GW-6 below.

Table GW-6

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.
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.

[11] NIST CSF at 9.

Function Name	Category Name	Category Description
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-7 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 "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-7

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 cybersecurity 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 cyber Security 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 cybersecurity. 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 cybersecurity activities and spending would not be beneficial to customers with respect to safe and reliable energy delivery and protecting sensitive customer information.

B. Safety Culture

SDG&E 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 electric and gas infrastructure, and providing safe and reliable

electric and 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.

C. Cybersecurity Program Summary

As discussed above, the Cybersecurity Program is a cross-cutting business function, which supports key SDG&E 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.

Cybersecurity activities and projects are vital to maintaining the safe, reliable delivery of energy, safeguarding customer information, complying with regulations, and protecting

[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.

technology assets and information. The following sections provide more detail on activities and projects, describe how they fit into the cybersecurity risk 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.

III. 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.

IV. 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) SDG&E or SoCalGas, (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 escalating costs associated with supporting the capital projects after their implementation. Additionally, difficulty recruiting and retaining cybersecurity staff led to lower recorded costs in 2016. The TY 2019 estimates for Security Engineering and Security Operations assume the allocated cybersecurity positions are filled for the entire year.

Table GW-8 below summarizes the total shared O&M forecasts for the listed cost categories.

TABLE GW-8

Shared O&M Summary of Costs

CYBERSECURITY (In 2016 $)			
(In 2016 $) Incurred Costs (100% Level)			
Categories of Management	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
A. SECURITY POLICY & AWARENESS	957	957	0
B. DIRECTOR - INFORMATION SECURITY	367	367	0
C. SECURITY ENGINEERING	992	1,434	442
D. SECURITY OPERATIONS	1,642	1,757	115
E. SECURITY CONTRACTS	2,587	3,370	783
G. INFORMATION SECURITY PROGRAMS	22	22	0
Total Shared Services (Incurred)	**6,567**	**7,907**	**1,340**

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. The O&M historical and forecast costs do not include costs associated with cost center 2100-3840 – Critical Infrastructure Protection, as they are FERC funded. Table GW-9 below summarizes the NIST CSF related activity supported by each of the cybersecurity teams.

Table GW-9
Summary of Cybersecurity Team Activities

Function Name	Category Name	Team				
		Director – Information Security and Information Security Programs	Security Policy and Awareness	Security Engineering	Security Operations	Security Contracts
IDENTIFY	Asset Management	Enabling function covering all the Identify capabilities	Establishes cybersecurity roles and responsibilities for the workforce and third party stakeholders			
IDENTIFY	Business Environment		Communicates the cybersecurity aspects of the business environment and the necessary resiliency requirements			
IDENTIFY	Governance		Develops and maintains the security policy framework, communicates requirements and responsibilities, and support cybersecurity risk management processes		Ensures legal and regulatory requirements regarding incidents are followed based upon policies and procedures	
IDENTIFY	Risk Assessment		Tracks potential business impacts and likelihoods of known risks	Identifies and tracks potential business impacts and the likelihoods of risks found while supporting system development and implementation projects	Identifies and tracks potential business impacts and likelihoods of risks found in the production environment or via threat intelligence	
IDENTIFY	Risk Management Strategy		Supports operational risks by utilizing the Company's priorities, constraints, risk tolerances, and assumptions			Supports the Company's goals of safety and reliability by funding the continued use and maintenance of vendor products to achieve cybersecurity risk management objectives
PROTECT	Access Control	Enabling function covering all the Protect capabilities	Provides access management for the NERC CIP environments	Designs network security and privileged account access controls		

Function Name	Category Name	Team				
		Director – Information Security and Information Security Programs	Security Policy and Awareness	Security Engineering	Security Operations	Security Contracts
PROTECT	Awareness and Training		Provides personnel and partners cybersecurity awareness education consistent with related policies, procedures, and agreements		Works with senior executives to ensure understanding of roles and responsibilities during an incident	
PROTECT	Data Security			Designs internal public key infrastructure, data loss prevention controls, and other data protection capabilities		
PROTECT	Information Protection Processes and Procedures		Shares effectiveness information with appropriate parties, and contributing to continuous improvement processes	Develops secure baselines, prepares incident response and recovery procedures for cybersecurity control technology, sharing effectiveness information with appropriate parties, and contributes to continuous improvement processes	Develops and implements vulnerability management plans, sharing information with appropriate parties, and contributes to continuous improvement processes	
PROTECT	Maintenance			Provides software patching services		
PROTECT	Protective Technology			Provides controls for network protection, logging functions, and configures access controls	Provides protection of networks, reviews logs, monitors system access, and detects anomalous activity	
DETECT	Anomalies and Events	Enabling function covering all the Detect capabilities			Develops baseline of expected data flows to detect anomalous events	
DETECT	Security Continuous Monitoring				Continuously monitors the information assets of the Company	
DETECT	Detection Processes				Defines, tests, communicates, and improves detection processes	
RESPOND	Response Planning	Enabling function covering all the Respond capabilities		Executes response plan for supported systems during an event	Executes response plans for supported systems during an event	
RESPOND	Communications				Coordinates internal communications during a cybersecurity incident	
RESPOND	Analysis		Provides cyber forensics services		Provides investigations, analyzes, and tracks	

Function Name	Category Name	Team				
		Director – Information Security and Information Security Programs	Security Policy and Awareness	Security Engineering	Security Operations	Security Contracts
					cybersecurity event notifications and incidents.	
RESPOND	Mitigation		Tracks risks associated with newly identified vulnerabilities	Tracks risks associated with identified vulnerabilities in new and supported systems	Responsible for mitigating cybersecurity incidents	
RESPOND	Improvements				Leads after-action activities for exercises and incidents	
RECOVER	Recovery Planning	Enabling function covering all the Recover capabilities		Executes recovery plans for supported systems during an event	Supports recovery activity as needed after an incident	
RECOVER	Improvements			Reviews and improves recovery plans for supported systems during an event	Leads the review and improvement of recovery plans after an incident	
RECOVER	Communications		Communicates with internal stakeholders and executive and management teams on recovery efforts		Communicates with internal stakeholders and executive and management teams on recovery efforts	

The Grid Modernization Projects that are focused on enhancing the cybersecurity of SDG&E's electric distribution system include the implementation of new systems. Expansion of existing cybersecurity capabilities to secure new systems does not increase maintenance costs.

B. Director – Information Security and Information Security Programs

TABLE GW-10

Summary of Costs – Director – Information Security

(In 2016 $) Incurred Costs (100% Level)			
B. DIRECTOR - INFORMATION SECURITY	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. DIRECTOR - INFORMATION SECURITY	367	367	0
Incurred Costs Total	**367**	**367**	**0**

TABLE GW-11

Summary of Costs – Information Security Programs

(In 2016 $) Incurred Costs (100% Level)			
G. INFORMATION SECURITY PROGRAMS	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. INFORMATION SECURITY PROGRAMS	22	22	0
Incurred Costs Total	**22**	**22**	**0**

1. Description of Costs and Underlying Activities

The Director of Information Security and the Information Security Program are an enabling function covering all the NIST CSF capabilities supported by Security Policy and Awareness, Security Engineering, Security Operations, and their respective capital projects at a management level.

The Director's activities include overall oversight of the Cybersecurity Program and projects, responsibility for cybersecurity at SDG&E, SoCalGas, and Corporate Center, advocating internally and externally for cybersecurity risk management, and representing cybersecurity in cross-business group activities. These activities include both labor and non-labor costs.

The Information Security Programs group is responsible for:

- Cybersecurity projects portfolio management, concepts, request for proposals (RFPs), and business case development.
- Cybersecurity projects planning and strategy.
- Cybersecurity O&M contracts and maintenance budget management.
- Cybersecurity vendor management.

These costs support the Company's goals of safety and reliability by directing, authorizing, and allocating resources to manage cybersecurity risks across the company.

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 for both the Director and the Information Security Program costs.

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 and mitigating cybersecurity risk as described in Section II above and in the RAMP Report. These drivers are consistent with California Public Utilities Commission (CPUC) and FERC requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

C. Security Policy and Awareness

TABLE GW-12

(Security Policy and Awareness)

(In 2016 $) Incurred Costs (100% Level)			
A. SECURITY POLICY & AWARENESS	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. SECURITY POLICY & AWARENESS	957	957	0
Incurred Costs Total	**957**	**957**	**0**

1. Description of Costs and Underlying Activities

The Security Policy and Awareness group's primary focus is on governance and compliance and the awareness and outreach aspects of the Cybersecurity Program. These activities include a combination of labor and non-labor costs.

The governance and compliance functions of the Cybersecurity Program provide security program strategy and oversight, a corporate security policy framework consisting of policies, standards, and guidelines, security risk management and exception tracking, project planning and portfolio management, security legislation and regulatory analysis, forensics, e-Discovery, and IT compliance associated with NERC CIP regulations.

The Cybersecurity Program's focus on awareness and outreach is designed to provide security-oriented training and communication to all Company employees through the use of newsletters, flyers, digital publications, town hall meetings, classroom and online training, and special events with cybersecurity experts. The activities, tools, and training used to improve cybersecurity awareness are as follows:

Activities:

- Cyber Champions - Internal groups throughout the various business units promoting cybersecurity safety/awareness.

- Town hall meetings - Lunch-n-learn, joint department presentations (Cybersecurity/Corporate Security), National Cybersecurity Awareness Month, etc.
- Classroom - Safety stand-downs, tailgates, department meetings, staff meetings, Cyber Champions training.

Tools:

- Internal webpage (iProtect) – All cybersecurity information is posted, made available to all employees.
- Internal mailbox (iProtect) – Mailbox where questions/concerns can be asked.
- Report Spam button – One-step way for employees to report suspicious emails.

Training:

- Anti-Phishing Training – Internal anti-phishing educational campaigns.
- Gamification – Interactive education mobile tool that behaves like games.
- Newsletters - SANS, etc.
- Posters/Flyers
- Digital publications - Articles, informational notifications, alerts, cybersecurity trending, tools enhancements, new tool/services cybersecurity deployments.
- Online training – Mandated compliance training (annual).
- Special events - Safety Congress.

The Security Policy and Awareness is organized into three teams:

- Security Policy and Awareness – Responsible for cybersecurity activities related to Education, Communications, Awareness, Cyber Champions Program, Policies, Regulatory review and commenting, Legislative support, maintenance and negotiation of contract language, Strategy, Architecture, and Risk Exceptions.
- Critical Infrastructure Protection (CIP) – Responsible for cybersecurity compliance with the NERC CIP reliability standards.
- Digital Investigations – Responsible for Litigation support, eDiscovery, Legal holds, Legal and human resources (HR) investigations, digital investigations, and Forensics.

The costs associated with the Security Policy and Awareness group support 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 identified in the RAMP Report and supports the NIST CSF capabilities by providing Identify, Protect, Respond, and Recover functionality as summarized in Table GW-13 below.

Table GW-13

Summary of Security Policy and Awareness Activities

Function	Category	Activities
Identify	Asset Management	Identifies the data, personnel, devices, systems, and facilities that enable the Company's business functions and ensures they are managed consistently with their relative importance to the business objectives and risk strategy. The group supports the capability by establishing cybersecurity roles and responsibilities for the workforce and third party stakeholders.
	Business Environment	Business Environment – specifies the Company's mission, objectives, stakeholders, and activities and uses this information to inform cybersecurity roles, responsibilities, and risk management decisions. The group is responsible for communicating the cybersecurity aspects of the business environment and the necessary resiliency requirements.
	Governance	Governance – tracks how other controls are functioning to rapidly escalate potential issues, to enable future improvements, and demonstrate compliance with regulatory requirements. The group also supports the security policy framework, communicates requirements and responsibilities, and support cybersecurity risk management processes.
	Risk Assessment	Risk Assessment – tracks and communicates cybersecurity risk to the Company's operations, assets, and individuals. The group supports this capability by tracking potential business impacts and likelihoods of known risks.
	Risk Management Strategy	Risk Management Strategy – uses the Company's priorities, constraints, risk tolerances, and assumptions to support operation risk decisions. The group provides this capability for cybersecurity risks.
Protect	Access Control	Access Control limits access to information and operation systems to authorized users, processes, or devices, and to authorized activities and transactions. Access Control also improves cybersecurity by preventing unauthorized users from viewing or manipulating systems or information. The group supports access management for the NERC CIP environment.
	Awareness and Training	Awareness and Training 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.
	Information Protection Processes and Procedures	Information Protection Processes and Procedures addresses adherence to policies and procedures to manage the protection of assets. This group also supports the human resources aspects of cybersecurity, sharing effectiveness information

Function	Category	Activities
		with appropriate parties, and contributing continuous improvement processes.
Respond	Analysis	Analysis is conducted to ensure adequate response and recovery activities. The group provides cyber forensics services in support of this capability.
	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.
Recover	Communications	Communications during recovery involve the coordination of multiple stakeholders that may be impacted. The group supports this capability via communications with internal stakeholders and executive and management teams.

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 and mitigating cybersecurity risk as described in Section II above and in the RAMP Report. These drivers are consistent with CPUC and FERC requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

D. Security Engineering

TABLE GW-14

(Security Engineering)

(In 2016 $) Incurred Costs (100% Level)			
C. SECURITY ENGINEERING	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. SECURITY ENGINEERING	992	1,434	442
Incurred Costs Total	**992**	**1,434**	**442**

1. Description of Costs and Underlying Activities

The Security Engineering group's primary focus is supporting projects to secure applications and systems before they are placed in production, and implementing, administering, and managing cybersecurity technologies. These activities include a combination of labor and non-labor costs.

The Security Engineering practice 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 and the controls necessary to mitigate those potential risks.

The Security Engineering group has three teams:

- Information Security (IS) Engineering & Consulting – Provides cybersecurity consulting services to SDG&E, SoCalGas, 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 – Supports enhanced access controls, Public Key Infrastructure, Data Loss Prevention, and endpoint security.

The costs associated with the Security Engineering group support 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 by providing Identify, Protect, Respond, and Recover functionality as summarized in Table GW-15 below.

Table GW-15

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	Access Control 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	Data Security protects information and data while it is at rest or in transit. This capability 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	Information Protection Processes and Procedures addresses adherence to policies and procedures to manage the protection of assets. The group provides support by developing secure baselines, preparing incident response and recovery procedures for cybersecurity control technology, sharing effectiveness information with appropriate parties, and contributing to continuous improvement processes.
	Maintenance	Maintenance allows for 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 identifies technical solutions that are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements. The group supports the protection of networks, reviews audit logs of the systems they support, and assists with business implementation projects by implementing logging functions and configuring access controls.
Respond	Response Planning	Response Planning oversees 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.

Function	Category	Activities
Recover	Recovery Planning	Recovery Planning oversees 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 and mitigating cybersecurity risk as described in Section II above and in the RAMP Report. Contract labor cost increase to reflect a full year of a contractor supporting operation and administration of cybersecurity systems. These drivers are supported by CPUC and FERC requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

E. Security Operations

TABLE GW-16

(Security Operations)

(In 2016 $) Incurred Costs (100% Level)			
D. SECURITY OPERATIONS	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. SECURITY OPERATIONS	1,642	1,757	115
Incurred Costs Total	**1,642**	**1,757**	**115**

1. Description of Costs and Underlying Activities

The Security Operations group has four teams:

- Security Operations Center (SOC) Engineering – Manages and maintains the centralized log collection, analysis, and alerting platform.
- Threat and Vulnerability Management – Responsible for vulnerability discovery, reporting, and tracking and threat intelligence collection and dissemination.

- Incident Response – Conducts incident investigations and analysis, threat-hunting, forensic analysis, malware analysis, and improves detective controls.
- Event Monitoring & Triage – 24x7 cybersecurity monitoring and analysis of security events, first line of support and coordination for incident response.

The teams are supported by an enterprise log analysis and event correlation solution, which consolidates information from multiple enterprise, infrastructure, and cybersecurity systems. Predefined correlation rules and queries present alerts to the Information Security Operations Center (ISOC) about possible malicious activity. Ad hoc monitoring and review for anomalous activity is also conducted. User reported cyber events and threat intelligence resources are also channeled through the ISOC. These activities include a combination of labor and non-labor costs.

The costs of the Security Operations group support the Company's goals of safety and reliability by maintaining and improving the cybersecurity posture by proactively detecting and minimizing the impact cybersecurity risks across the Company. These costs are shared for efficient use of specialized staff and infrastructure. These costs were included in the RAMP Report and support the NIST CSF capabilities by providing Identify, Protect, Detect, Respond, and Recover functionality in the production environments as summarized in Table GW-17 below.

Table GW-17

Summary of Security Operations Activities

Function	Category	Activities
Identify	Governance	Governance controls support cybersecurity by tracking how other controls are functioning to rapidly escalate potential issues, enable future improvements, and demonstrate compliance with regulatory requirements. The group is responsible for ensuring legal and regulatory requirements regarding incidents are followed based on policies and procedures.
	Risk Assessment	Risk Assessment supports 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 in the production environment or via threat intelligence.
Protect	Awareness and Training	Awareness and Training provides personnel and partners with cybersecurity awareness education to adequately train them to perform their cybersecurity-related duties and responsibilities

Function	Category	Activities
		consistent with related policies, procedures, and agreements. The group works with senior executives to ensure they understand their roles and responsibilities during an incident.
	Information Protection Processes and Procedures	Information Protection Processes and Procedures addresses adherence to policies and procedures to manage the protection of assets. The group provides support by developing and implementing vulnerability management plans, sharing information with appropriate parties, and contributing to continuous improvement processes.
	Protective Technology	Protective Technology are technical solutions that are managed to ensure the security and resilience of systems and assets are consistent with related policies, procedures, and agreements. The group supports the protection of networks, reviews logs, and monitors access to system to detect anomalous activity.
Detect	Anomalies and Events	Anomalies and Events analyzes collected information to find anomalous cybersecurity activity that requires either further investigation or incident response actions. The group uses a baseline of expected data flows to detect anomalous events to analyze to determine if an incident is in progress.
	Security Continuous Monitoring	Security Continuous Monitoring is the gathering of information of activity and vulnerability status from multiple resources. The group is responsible for continuously monitoring the information assets of the Company.
	Detection Processes	Detection Processes are maintained and tested to ensure timely and adequate awareness of anomalous events. The group is responsible for defining, testing, communicating, and improving the detection process.
Respond	Response Planning	Response Planning oversees 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.
	Communications	Communications ensures response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. The group coordinates internal communications during a cybersecurity incident.
	Analysis	Analysis is conducted to ensure adequate response and recovery activities. The group investigates, analyzes, and tracks cybersecurity event notifications and incidents.
	Mitigation	Mitigation activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. The group is responsible for mitigating cybersecurity incidents.
	Improvements	Improvements seek to improve organizational response activities by incorporating lessons learned from current and previous detection/response activities. The group leads after action activities for exercises and incidents.
Recover	Recovery Planning	Recovery Planning oversees the execution of the recovery plan during or after an event. The group supports recovery activity as needed after an incident.

Function	Category	Activities
	Improvements	Improvements uses lessons learned during recovery planning and processes in future activities. The group leads review and improvement of recovery plans after an incident.
	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.

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 and mitigating cybersecurity risk as described Section II above and in the RAMP Report. Labor cost increase is due to the addition of one FTE required as additional staff to provide support of security operations. These drivers are consistent with CPUC and FERC requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

F. Security Contracts

TABLE GW-18

(Security Contracts)

(In 2016 $) Incurred Costs (100% Level)			
E. SECURITY CONTRACTS	**2016 Adjusted-Recorded (000s)**	**TY 2019 Estimated (000s)**	**Change (000s)**
1. SECURITY CONTRACTS	2,587	3,370	783
Incurred Costs Total	**2,587**	**3,370**	**783**

1. Description of Costs and Underlying Activities

Security Contracts are non-labor expenses that include maintenance costs and licensing for historical and planned capital projects at SDG&E, SoCalGas, and Corporate Center. This cost supports the Company's goals of safety and reliability by funding the continued use and maintenance of vendor products to achieve cybersecurity risk management objectives. These

costs are shared for efficient use of specialized infrastructure and were included in the RAMP Report.

2. Forecast Methodology

The forecast methodology developed for this cost category is zero-based. This method is most appropriate because the O&M costs are non-labor costs associated with product licensing and support for existing implementations and in support of the Grid Modernization Projects.

3. Cost Drivers

The cost drivers behind this forecast are due to increasing maintenance and licensing costs related to historical and planned capital projects. These projects are necessary to address evolving threat actor capabilities as well to enable new technology use cases within the IT/Operational Technology (OT) environment. In addition, mitigating cybersecurity risk as described in Section II above and in the RAMP Report is another contributing factor to the increase. These drivers are supported by CPUC and FERC requirements, California and Federal statutes, and Company policy. These costs were identified in the RAMP filing.

V. 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 because of the continuous reassessment of threats, known risks, and prioritization.

The capital projects set forth in Table GW-19 below each support different NIST CSF Functions and Categories. Some projects may appear to overlap since a single project does not address all the sub-capabilities or applicable assets/services, and some projects implement multiple capabilities. The addressed NIST CSF elements are described in more detail for each project below.

Table GW-19

Summary of Capital Projects and Applicable NIST CSF Function/Categories

Function Name	Category Name	Project Name
IDENTIFY	Asset Management	
IDENTIFY	Business Environment	
IDENTIFY	Governance	Compliance Records Management
IDENTIFY	Risk Assessment	
IDENTIFY	Risk Management Strategy	
PROTECT	Access Control	Critical Infrastructure Protection Smart Grid Substation Gateway Security Phase 2 Electric Distribution Operations Network Security Architecture Redesign and Upgrade Electric Distribution Directory Services Electric Distribution Multifactor Authentication Electric Distribution RTU Password and Configuration Management Electric Distribution Privileged Access Management
PROTECT	Awareness and Training	
PROTECT	Data Security	Critical Infrastructure Protection Field Area Network Security
PROTECT	Information Protection Processes and Procedures	Electric Distribution RTU Password and Configuration Management
PROTECT	Maintenance	Compliance Records Management Critical Infrastructure Protection Smart Grid Substation Gateway Security Phase 2
PROTECT	Protective Technology	Critical Infrastructure Protection Smart Grid Substation Gateway Security Phase 2 Electric Distribution Operations Network Security Architecture Redesign and Upgrade Field Area Network Security Electric Distribution Privileged Access Management
DETECT	Anomalies and Events	Critical Infrastructure Protection Network Anomaly Detection Phase 3 Electric Distribution Operator End Point Protection
DETECT	Security Continuous Monitoring	Critical Infrastructure Protection Network Anomaly Detection Phase 3 Electric Distribution Operator End Point Protection
DETECT	Detection Processes	
RESPOND	Response Planning	
RESPOND	Communications	
RESPOND	Analysis	
RESPOND	Mitigation	
RESPOND	Improvements	
RECOVER	Recovery Planning	
RECOVER	Improvements	
RECOVER	Communications	

Table GW-20 below summarizes the total capital forecasts for 2017, 2018, and 2019 for the capital projects discussed in the following sections based on the related NIST CSF function.

TABLE GW-20

Capital Expenditures Summary of Costs
(Thousands of Dollars)

Project Type	Project Name	2017	2018	2019
Identify	Compliance Records Management	876	-	-
Identify Total		**876**	**-**	**-**
Protect	Critical Infrastructure Protection	1,428	1,842	2,270
Protect	Smart Grid Substation Gateway Security Phase 2	1,068	1,332	1,416
Protect	Distribution Operations Multifactor Authentication	580	580	
Protect	Distribution RTU Password and Configuration Mgmt		387	386
Protect	Privilege Access Manager		772	772
Protect	EDO Network Security Architecture Redesign	772	772	
Protect	Active Directory Domain Controllers for Distribution	386	386	
Protect	Field Area Network Security		775	774
Protect Total		**4,234**	**6,846**	**5,618**
Detect	Network Anomaly Detection Phase 3	110	-	-
Detect	Distribution End Point Protection	926	386	
Detect Total		**1,036**	**386**	**-**
Cyber Security Total		**6,146**	**7,232**	**5,618**

The Grid Modernization Projects that are focused on improving the cybersecurity of SDG&E's electric distribution system, which are discussed in the testimony of Alan Colton (Ex. SDG&E-14), and the associated total capital forecasts for 2017, 2018, and 2019, which I am sponsoring, are identified and summarized in Table GW-21 below.

TABLE GW-21

Capital Expenditures Summary of Costs in Support of the Grid Modernization Projects
(Thousands of Dollars)

Project Type	Project Name	2017	2018	2019
Grid Modernization	Distribution Operations Multifactor Authentication	580	580	-
Grid Modernization	Distribution End Point Protection	926	386	-
Grid Modernization	Distribution RTU Password and Configuration Mgmt	-	387	386
Grid Modernization	Privilage Access Manager	-	772	772
Grid Modernization	EDO Network Security Architecture Redesign	772	772	-
Grid Modernization	Active Directory Domain Controllers for Distribution	386	386	-
Grid Modernization	Field Area Network Security	-	775	774
Program Total		**2,664**	**4,058**	**1,932**

B. Compliance Records Management (Identify)

1. Description

The forecast for the Compliance Records Management project for 2017 is $876,000. SDG&E plans to build and place this project in service by the test year. This project will implement a solution designed to meet NERC CIP specific recording and reporting on CIP system controls. The NERC CIP requirements for information formats, templates, and retention schedules are not addressed by existing document management solutions. The specific details regarding the Compliance Records Management project are found in my capital workpapers. See Ex. SDG&E-25-CWP.

The project includes purchasing new software, hardware costs, and labor costs to design, implement, 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 complying with NERC CIP requirements. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-19 above by providing Governance capabilities under the Identify Function. Governance controls support cybersecurity by tracking how other controls are functioning to rapidly escalate potential issues, to enable future improvements, and demonstrating compliance with regulatory requirements.

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 the assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost driver for this capital project is maintaining compliance with NERC CIP requirements. Documentation of this cost driver is included in my capital workpapers. See Ex. SDG&E-25-CWP.

C. Critical Infrastructure Protection (Protect)

1. Description

The forecast for the Critical Infrastructure Protection project for 2017, 2018, and 2019 is $1,428,000, $1,842,000, and $2,270,000, respectively. SDG&E 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 and will 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 Critical Infrastructure Protection project are found in my capital workpapers. See Ex. SDG&E-25-CWP.

This project includes 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 them into service. 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 infrastructure. This project was included in the RAMP Report and supports the NIST CSF capabilities by providing both Protective and Detective functionality as summarized in Table GW-22 below.

Table GW-22

Summary of Critical Infrastructure Protection Project Activities

Function	Category	Activities
Protect	Access Control	Access Control 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.
	Data Security	Data Security 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	Maintenance 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 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	Anomalies and Events 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 of activity and vulnerability status from multiple resources.

2. Forecast Methodology

The forecast methodology developed for this cost category is a 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 enable 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. SDG&E-25-CWP.

D. Smart Grid Substation Gateway Security Phase 2 (Protect)

1. Description

The forecast for the Smart Grid Substation Gateway Security Phase 2 capital project for 2017, 2018, and 2019 is $1,068,000, $1,332,000, and $1,416,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will implement a solution designed to replace failing or insufficient gateway hardware by implementing network gateway devices to protect internet protocol (IP) networks within the substation to securely perform configuration management remotely. They also provide password management capabilities.

The specific details regarding the Smart Grid Substation Gateway Security Phase 2 project are found in my capital workpapers. See Ex. SDG&E-25-CWP. The project includes purchasing hardware, and labor costs to configure, install, and integrate the gateways in electric distribution substations.

The forecasted capital expenditures for this project support the Company's goals for safety and reliability by implementing security controls to manage cybersecurity risks while enabling remote access support for control operations. This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities by providing the Protect capabilities: Access Control, Protective Technology, and Maintenance as summarized in Table GW-23 below.

Table GW-23

Summary of Smart Grid Substation Gateway Security Project Activities

Function	Category	Activities
Protect	Access Control	Access Control 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.
	Protective Technology	Maintenance capability allows prompt maintenance and repair of company assets in a control 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.
	Maintenance	Protective Technology 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. The gateway prevents direct access to IP based devices in the substations.

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 the assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to IP-based devices that are a new technology being deployed into substations and to replace existing devices which are no longer suitable for this function. The gateways implement cybersecurity controls in the substation to reduce the likelihood of unauthorized access and the resulting impact to safety and reliability. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

E. Network Anomaly Detection Phase 3 (Detect)

1. Description

The forecast for the Network Anomaly Detection Phase 3 project for 2017 is $110,000. This project started in 2016 and SDG&E plans to continue to build and place this project in service by the test year. SDG&E is expanding IP-based communications and establishing substation local area networks (LANs) and field area networks (FANs) to support a variety of projects such as condition-based maintenance, substation physical security enhancements, and advanced SCADA devices. These new IP networks will support the next-generation distributed energy resources and SCADA device technologies, which are critical in maintaining the availability and security of the SDG&E electric grid.

Network Anomaly Detection technology provides SDG&E's cybersecurity team with a new level of situational awareness in networks never monitored previously, and provides SDG&E's Operational Technology groups a deeper level of visibility into the process they monitor and support. Network security monitoring is the top active defense mechanism recommended by industry experts after the Ukraine distribution utility cyber incident. The Network Anomaly Detection Phase 3 project will continue deployment of the solution to the identified facilities. The specific details regarding are found in my capital workpapers. See Ex. SDG&E-25-CWP.

The project includes purchasing new software, hardware costs, and labor costs to design, implement, 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 limiting the impact of cybersecurity incidents on the electric grid and potentially reducing the recovery time and duration of a cybersecurity event because the solution adds the ability to identify indicators of compromise within SDG&E's most critical networks/grid environments, a new capability to detect, respond and recover from a cyber incident in critical SDG&E SCADA serial networks, Electric Transmission & Distribution (T&D) Operators visibility into infrastructure configuration and performance, network operations visibility into network flows, and an analytic platform to provide ability to visualize network flows, security or misconfigurations.

This project was included in the RAMP Report as RAMP-Post Filing and supports the NIST CSF capabilities specified in Table GW-19 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 the assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to evolving threats such as those responsible for the Ukraine incident. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

F. Electric Distribution Operations (EDO) Network Security Architecture Redesign (Protect)

1. Description

The forecast for the Electric Distribution Operations (EDO) Network Security Architecture Redesign project for 2017 and 2018 is $772,000 and $772,000, respectively. SDG&E plans to build and place this project in service by the test year. This project is to redesign and upgrade the EDO network security architecture. The activities include consolidating firewall and intrusion prevention systems (IPS) into a single platform. The network architecture

of the Outage Management System (OMS)/Distribution Management System (DMS) will also be reviewed and updated based on the review. The specific details regarding the EDO Network Security Architecture Redesign project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, is provided in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes purchasing new software, hardware costs, and labor costs to design, implement, integrate the solution with related systems, and to test the functionality of the updated system before putting it into service. The forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining the cybersecurity posture of the electric distribution system as more automation is added to the system. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect capabilities of Access Control 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 redesigns and updates the electric distribution operations environment to improve network access controls for users and other applications, such as OMS/DMS.

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. This project improves control network protections.

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 the assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to refreshing technology to leverage updated product capabilities and support the implementation of new technologies related to the Grid Modernization Projects. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

G. Active Directory Domain Controllers for Distribution (Protect)

1. Description

The forecast for the Active Directory Domain Controllers for Distribution project for 2017 and 2018 is $386,000 and $386,000, respectively. SDG&E plans to build and place this project in-service by the test year. This project will implement Microsoft Active Directory Domain Controllers for the Electric Distribution control network. The specific details regarding this project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, is provided in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes purchasing new software, hardware costs, and labor costs to design, implement, migrate existing systems, 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 maintaining the cybersecurity posture of the electric distribution system as more automation is added to the system. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect 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.

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 reducing cybersecurity risk in support of the implementation of new technologies related to the Grid Modernization Projects. A significant part of this effort will be to migrate OMS/DMS to the new Active Directory solution. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

H. Distribution Operations Multifactor Authentication (Protect)

1. Description

The forecast for the Distribution Operations Multifactor Authentication project for 2017 and 2018 is $580,000 and $580,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will implement multifactor authentication hardware and software for all Electric Distribution Operations, operator workstations, and server assets. The specific details regarding the Distribution Operations Multifactor Authentication project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, are found in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes 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 forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining the cybersecurity posture of the electric distribution system as more automation is added to the system. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect capability of Access Control. 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.

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 the assets and tasks needed for implementation.

3. Cost Drivers

The underlying cost drivers for this capital project relate to reducing cybersecurity risk in support of the implementation of new technologies related to the Grid Modernization Projects. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

I. Distribution RTU Password and Configuration Management (Protect)

1. Description

The forecast for the Distribution Remote Terminal Units (RTU) Password and Configuration Management project for 2018 and 2019 is $387,000 and $386,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will implement centralized RTU password and configuration management for Electric Distribution substations. The specific details regarding the Distribution RTU Password and Configuration Management project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, are found in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes 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 forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining the cybersecurity posture of the electric distribution field RTUs. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect capabilities of Access Control and Information Protection Processes and Procedures.

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. 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.

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 reducing cybersecurity risk in support of the implementation of new technologies related to the Grid Modernization Projects.

Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

J. Field Area Network Security (Protect)

1. Description

The forecast for the Field Area Network Security project for 2018 and 2019 is $775,000 and $774,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will implement additional Field Area Network Security cybersecurity controls. The specific details regarding the Field Area Network Security project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, are found in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes 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 forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining the cybersecurity posture of the field network portions of the electric distribution system as more automation and new technologies are added. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect capabilities of Data Security and Protective Technology.

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. This project improves network security to protect data in transit. 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 focuses on protecting communications and control networks, logging, and managing the device network access.

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 reducing cybersecurity risk in support of the implementation of new technologies in field area networks related to the Grid Modernization Projects. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

K. Privileged Access Management (Protect)

1. Description

The forecast for the Privileged Access Management project for 2018 and 2019 is $772,000 and $772,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will implement a hardware/software privilege access manager for Electric Distribution Operations server and field assets. The specific details regarding the Privileged Access Management project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, is found in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes 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 forecasted capital expenditures for this project support the Company's goals for safety and reliability by maintaining the cybersecurity posture of the electric distribution system as more automation and technologies are added to the system. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Protect capabilities of Access Control and Protective Technologies.

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. 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.

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 reducing cybersecurity risk in support of the implementation of new technologies in the control network and field area networks related to the Grid Modernization Projects. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

L. Distribution End Point Protection (Detect)

1. Description

The forecast for the Distribution End Point Protection project for 2017 and 2018 is $926,000 and $386,000, respectively. SDG&E plans to build and place this project in service by the test year. This project will update end point protection on operator workstations and servers. The specific details regarding the Distribution End Point Protection project are found in my capital workpapers. See Ex. SDG&E-25-CWP. A broader discussion of the Grid Modernization Projects, which this project supports, is found in the testimony of Alan Colton (Ex. SDG&E-14).

The project includes purchasing new software, hardware costs, and labor costs to design, implement, and 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 maintaining the cybersecurity posture of the electric distribution system. This project supports the NIST CSF capabilities specified in Table GW-19 by providing the Detect capabilities of Security Continuous Monitoring and Anomalies and Events.

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

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 reducing cybersecurity risk in support of the implementation of new technologies in the control network and field area

networks related to the Grid Modernization Projects. Documentation of these cost drivers is included in my capital workpapers. See Ex. SDG&E-25-CWP.

VI. CONCLUSION

These forecasts are expected to allow SDG&E 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.

VII. 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 joining Sempra Energy, 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

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

DMS: Distribution Management System

DDoS: Distributed Denial of Service

EDO: Electric Distribution Operations

FAN: Field Area Networks

FERC: Federal Energy Regulatory Commission

FTE: Full-Time Equivalent

GRC: General Rate Case

HR: Human Resources

IP: Internet Protocol

IPS: Intrusion Prevention Systems

IS: Information Security

ISOC: Information Security Operations Center

IT: Information Technology

LAN: Local Area Network

NERC: North American Electric Reliability Corporation

NIST: National Institute of Standards and Technology

O&M: Operations and Maintenance

OMS: Outage Management System

OT: Operational Technology

R&D: Research and Development

RAMP: Risk Assessment Mitigation Phase

RFP: Request for Proposal

RTU: Remote Terminal Units

SCADA: Supervisory Control and Data Acquisition

SDG&E: San Diego Gas & Electric Company

SOC: Security Operations Center

SoCalGas: Southern California Gas Company

T&D: Transmission & Distribution

TY: Test Year

UPG: Ukrainian Power Grid