BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

Application of SOUTHERN CALIFORNIA GAS COMPANY (U 904 G) for Review of its Safety Model Assessment Proceeding Pursuant to Decision 14-12-025.	Application No. 15-05-___ (Filed May 1, 2015)

PREPARED DIRECT TESTIMONY OF
SCOTT KING
ON BEHALF OF SOUTHERN CALIFORNIA GAS COMPANY

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

May 1, 2015

#296429

TABLE OF CONTENTS

I. OVERVIEW AND PURPOSE 1

II. CYBERSECURITY RISK MANAGEMENT PROCESS 1

A. Cybersecurity Risk Assessment Methodology 2

B. Cybersecurity Capability Maturity Modeling 4

i. Current State 4

ii. Link to Cyber Risk Assessment Methodology 4

iii. Risk Assessment Drives Cybersecurity Investment Strategy 4

C. Measuring Performance Using Key Risk Indicators 5

III. LINK TO EVOLVING THREAT STATE 5

IV. IMPORTANCE OF VULNERABILITY MANAGEMENT AND INCIDENT RESPONSE AS SECURITY CONTROLS 6

V. ROLE OF CPUC 6

VI. CONCLUSION 7

VII. WITNESS QUALIFICATIONS 8

PREPARED DIRECT TESTIMONY OF
SCOTT KING
ON BEHALF OF SOUTHERN CALIFORNIA GAS COMPANY

I. OVERVIEW AND PURPOSE

Southern California Gas Company ("SoCalGas") established its Information Security Program ("IS Program") in 2001. From the advent of the program the core objective was, and continues to be, the protection of data, information systems, and critical infrastructure. Among the top priorities is enabling cybersecurity governance through robust standards and policies contained within an overarching Security Policy Framework that establishes:

- Best practices,
- Acceptable use policies,
- Information system security standards, and
- Provides Information and Operational Technology requirements for managing and maintaining technology systems.

Each of these components is based on standards, such as those published by the National Institute for Standards and Technology ("NIST") and the International Organization for Standardization ("ISO"). Additionally, California state laws, California Public Utilities Commission ("CPUC") directives, and federal regulatory requirements, such as the North American Electric Reliability Corporation Critical Infrastructure Protection Standards ("NERC CIP") and the Sarbanes-Oxley Act ("SOX"), have significantly influenced the core requirements of the IS Program. This combined approach allows SoCalGas to not only ensure we are following cybersecurity standards and best practices, but also meeting or exceeding the governance structures established by the legislature and other regulatory bodies.

II. CYBERSECURITY RISK MANAGEMENT PROCESS

The process for identifying and evaluating cybersecurity risk is aligned with the broader SoCalGas risk management process. As described in more detail by witness Jorge DaSilva , this process has six distinct steps:

a. Risk identification;

b. Risk analysis;

c. Risk evaluation and prioritization using a 7x7 matrix;

d. Mitigation plan development;

e. Allocation of funds; and

f. Monitoring and review

A. Cybersecurity Risk Assessment Methodology

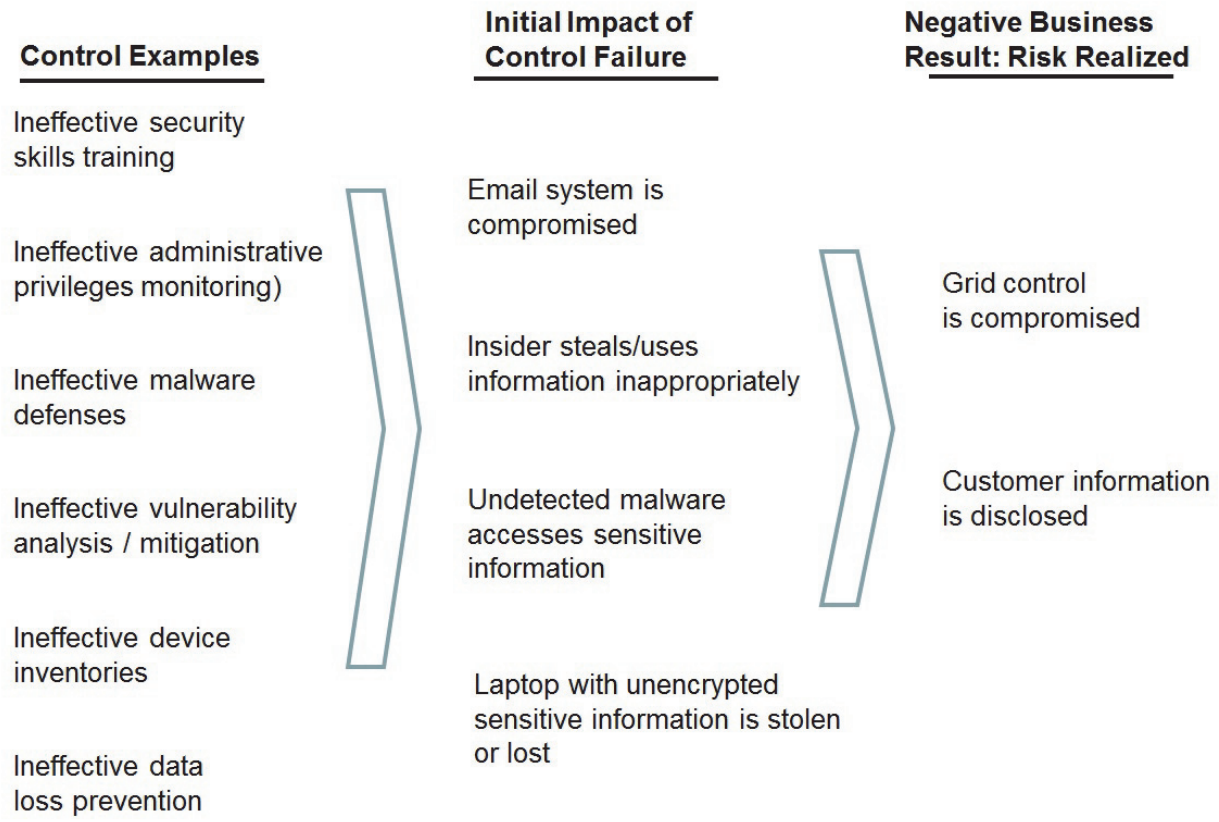
In accordance with ISO 31000, risk assessment includes risk identification, risk analysis and risk evaluation and prioritization (Steps 1 through 3 above). SoCalGas leverages two primary components in assessing cybersecurity risk:

- An enterprise Information Technology ("IT") risk register based on the Information Systems Audit and Control Association ("ISACA") Risk IT framework, and
- An industry recognized cybersecurity control framework incorporating 20 control categories.

Utilizing these two models, cybersecurity risk in the enterprise risk register can be expanded into specific risks based on 20 control categories to enable a deeper assessment of individual cybersecurity risks associated with cyber security control failures.

An initial analysis of cybersecurity risks provides a deeper understanding of the causes and effects of control failures. Table 1 below provides a visual example of this analysis:

TABLE 1



Based on the understanding of causes and effects of cybersecurity risks associated with control failures, risks are then evaluated using a 7x7 scale in three areas:

1. Strength of control;
2. Likelihood of control failure; and
3. Impact of control failure.

The scale itself takes into account safety, financial, and operational impacts defined by the companies Enterprise Risk Management methodology. This approach allows SoCalGas to broadly represent corporate cybersecurity risks, while at an operational level determine which cybersecurity controls must exist to inform investment priorities.

The cybersecurity control categories allow the IS Program to make informed decisions and provide company leadership risk details that enable prioritization of security investments that extend beyond the IS program into other business divisions. This enables further refinement of

risk based decision making for investments into critical infrastructure, customer privacy, business services, and financial systems.

B. Cybersecurity Capability Maturity Modeling

i. Current State

The Department of Energy ("DOE"), in partnership with Carnegie Melon and many other industry experts, developed a tool referred to as the Cybersecurity Capability Maturity Model or C2M2. The model enables the evaluation of a cybersecurity program against a defined, measurable set of best practices that directly map to escalating levels of maturity. Using this tool as a guide, a company can focus in on the cybersecurity areas most important to their business and understand where strengths and improvement opportunities exist. The tool allows for an extreme amount of flexibility in that a company can choose to model specific lines of business or the company overall. Using this format, reports are generated that can be easily digested by management to help visually depict the maturity of 10 key cybersecurity domains based on a 1-3 rating, with 3 as the most mature.

ii. Link to Cyber Risk Assessment Methodology

Evaluating the capability and maturity of a cybersecurity program is an important component of understanding business risk. These components should be used to influence how cyber security control categories are assessed, which builds a risk picture, and allow an organization to prioritize a multi-year investment strategy.

The C2M2 is a great example where several different risk assessment methodologies can be mapped directly to the maturity model and be used to drive risk ratings across cybersecurity control, and ultimately business risk.

iii. Risk Assessment Drives Cybersecurity Investment Strategy

Aligning the cybersecurity investment strategy to a risk management framework and a maturity model, allows an organization to develop a multi-year strategy for both operational and capital investments. These investments can include additional people, updated or new technology, and process improvement. The assessments are key to understanding what is working and where opportunities exist.

C. Measuring Performance Using Key Risk Indicators

Closely related to assessing cybersecurity risk from control categories, metrics provide a means to measure ongoing performance of investments. While many operational metrics are collected to measure the functionality of specific control technology, a compressed view is represented to company leadership in the form of Key Risk Indicators. Key Risk Indicators measure operational activity related to cybersecurity threats, susceptibility of technology assets, and performance of core security control processes such as vulnerability management and incident response. The actual metrics evolve to leverage industry best practices and organizational experiences.

Each of these measurements enables the ongoing assessment of the current cybersecurity risk as they relate to control failures. While the failures themselves are not a direct indication of risk, they do represent where commercial technology does not mitigate constantly evolving cybersecurity threats and help determine where additional investment into resources (technology, research, and people) is needed.

III. LINK TO EVOLVING THREAT STATE

In 2014, the United States Computer Emergency Readiness Team ("US-CERT") alerted the nation to 7937 new, previously unknown, vulnerabilities from the National Vulnerability Database ("NVD"). Looking back historically, that represents a year by year increase of approximately 38% since 2005 for all categories (Low-Critical).

To the cybersecurity industry as a whole, the challenge is at an all-time high as a national lack in skilled workforce and aging cybersecurity control technology struggle to keep up with the increasing rate of new methods, techniques, and tactics employed by our nation's adversaries. This requires industries of all types to make investments into research and development in order to evolve the cybersecurity capabilities of our nation.

From a utility perspective, this presents an additional challenge in the sense that Industrial Control Systems are continuing to evolve and expand into new areas that allow our industry to provide real-time monitoring of grid infrastructure, more flexibility in energy generation sources, and improved customer visibility of energy usage, among others. While these advancements are incredibly beneficial to the industry and our customers, they also have the side effect of further expanding the number of technology systems, increasing the use of

current generation communication technologies, and ultimately provide additional targeting opportunities for the adversaries.

Managing these risks is critical in the short term to ensure our industry is making the right decisions to protect the assets and data most important for our company and our customers.

As cybersecurity threats evolve, there will be a continuous need for our processes and methodologies to evolve in order to address new trends in cybersecurity risks.

IV. IMPORTANCE OF VULNERABILITY MANAGEMENT AND INCIDENT RESPONSE AS SECURITY CONTROLS

Two of the most important capabilities all companies should have in its cybersecurity toolbox are a vulnerability management program and an incident response team. A robust vulnerability management process will consist of four primary components: skilled resources, the ability and tools to assess for weaknesses in software and infrastructure, a mechanism for tracking and reporting deficiencies in the organization's technology assets, and executive management support for prompt patching and mitigation.

Incident response is similar, but contains slightly different components: skilled resources, a mechanism for tracking and reporting, and executive management support are equally as critical but the one item that is most often overlooked with regards to incident response, is the ability and tools to hunt for, detect, and respond to security events as quickly as possible.

When both of the aforementioned controls are operating effectively, the organization can do a much better job assessing risk and reducing the risk impact of a potential control failure.

V. ROLE OF CPUC

The CPUC is critical to the successful management of cybersecurity risk and investment strategies for the Investor-owned Utilities ("IOUs") within the state. The IOUs, and CPUC alike, share the same objective and desire to maintain safe and reliable energy infrastructure that protects the privacy of customers. Through risk management, those objectives can be assessed and discussed in terms that align with California law and the best interest of the utility's ratepayers.

There are however some situations where additional scrutiny is required to fully understand the risk introduced through vulnerabilities and threats. In those situations, the IOUs must be able to ensure the confidentiality of the information shared. That confidentiality is

critical to allowing the IOUs to openly share details that would result in system stability and data confidentially issues should an adversary become knowledgeable of the underlying weaknesses. Current confidentiality protections are in place to help, but additional thought and debate is needed to balance the desire to know versus the need to know.

VI. CONCLUSION

Information Security is a core business practice that allows SoCalGas to make informed decisions regarding cybersecurity risk. The risk profile, determined through risk modeling, and the maturity model, determined through capability assessments, allows SoCalGas to understand how cybersecurity risk applies to every aspect of its business. This understanding provides insight into where the company needs to operate strong controls and have a very small risk profile, and where more risk may be acceptable. These efforts represent both short term tactical risk as well as long term strategic risk.

Short term cybersecurity risks are those that can be corrected in a minimal amount of time with very little investment. Treatment mechanisms such as compensating controls, where a safeguard is leveraged to protect an asset, risk exceptions, where risk is acknowledged and temporarily accepted, or risk remediation where risk is significantly minimized or nearly eliminated are preferred.

Long term cybersecurity risks are those that take significantly longer to remediate and generally involve some level of investment. These risks are critical to assess and understand so a strategy to manage them can be developed. The strategy typically consists of a temporary risk exception, to document and track the risk over time, and a project concept or business case to demonstrate the need for risk reduction through investment.

Managing both short and long term cybersecurity risks are equally important. Without understanding where risks exist, what treatment options are available, and putting a plan in place to manage them, the organization is not making fully informed business decisions.

This concludes my prepared direct testimony.

VII. WITNESS QUALIFICATIONS

My name is Scott King and I currently serve as the Manager of Information Security for Southern California Gas Company, San Diego Gas and Electric Company, and Sempra Energy. My business address is 8335 Century Park Ct, San Diego CA 92123.

I have worked as an information security subject matter expert for approximately 15 years. In my current role, I am responsible for the management of the company's information security department. I have been a member of the department since 2008 and have held multiple positions.

Prior to my current employment, I worked for a major cyber security company, where I provided expert consulting services to large and small commercial/government entities. Prior to that I worked as a contractor supporting the Department of Defense.

I have not previously testified before the California Public Utilities Commission.