

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

Application of SAN DIEGO GAS & ELECTRIC
COMPANY (U 902 M) 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 SAN DIEGO GAS & ELECTRIC COMPANY**

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

May 1, 2015



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

- 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). SDG&E 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:

1

TABLE 1

<u>Control Examples</u>	<u>Initial Impact of Control Failure</u>	<u>Negative Business Result: Risk Realized</u>
Ineffective security skills training	Email system is compromised	Grid control is compromised
Ineffective administrative privileges monitoring)	Insider steals/uses information inappropriately	Customer information is disclosed
Ineffective malware defenses	Undetected malware accesses sensitive information	
Ineffective vulnerability analysis / mitigation	Laptop with unencrypted sensitive information is stolen or lost	
Ineffective device inventories		
Ineffective data loss prevention		

2

3 Based on the understanding of causes and effects of cybersecurity risks associated with

4 control failures, risks are then evaluated using a 7x7 scale in three areas:

- 5 1. Strength of control;
- 6 2. Likelihood of control failure; and
- 7 3. Impact of control failure.

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

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

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

3 **B. Cybersecurity Capability Maturity Modeling**

4 **i. Current State**

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

15 **ii. Link to Cyber Risk Assessment Methodology**

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

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

23 **iii. Risk Assessment Drives Cybersecurity Investment Strategy**

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

29

1 **C. Measuring Performance Using Key Risk Indicators**

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

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

15 **III. LINK TO EVOLVING THREAT STATE**

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

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

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

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

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

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

7 **IV. IMPORTANCE OF VULNERABILITY MANAGEMENT AND INCIDENT** 8 **RESPONSE AS SECURITY CONTROLS**

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

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

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

21 **V. ROLE OF CPUC**

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

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

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

5 **VI. CONCLUSION**

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

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

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

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

26 This concludes my prepared direct testimony.

27

1 **VII. WITNESS QUALIFICATIONS**

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

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

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

12 I have not previously testified before the California Public Utilities Commission.
13