ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

Exhibit Reference: SCG-18

Subject: IT Cybersecurity

Please provide the following:

1. Please provide SCG's policy governing cybersecurity.

SoCalGas Response 01:

SoCalGas policy governing cybersecurity are listed as part of the Information Security Acceptable Use Policy (ORA-SCG-DR-040-PM1 Q1 Attachment A) and the Information Security Standard/Procedure (ORA-SCG-DR-040-PM1 Q1 Attachment B).

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

2. Please provide a list of each cybersecurity related capital project SDG&E has requested funding for in the TY 2008, TY 2012 and TY 2016 GRCs with the following information:
    a. Yearly funding requested (in nominal and test year 2013 dollars).
    b. Scope of project.
    c. Intention of project.
    d. If SDG&E conducted cost to benefit studies, please provide copies of the studies.
    e. Copies of direct testimony and supporting workpapers.
    f. Actual recorded spending by year, delineated by capital expenditures and O&M expenses and further by labor and non-labor (in nominal and test year 2013 dollars).

SDG&E Response 02:

A. Please see attachment ORA-SDG&E-DR-036-PM1 Q2 A-C & E-F for information concerning the yearly funding requested in nominal and test year 2013 dollars.

B. Please see attachment ORA-SDG&E-DR-036-PM1 Q2 A-C & E-F for a list of the projects as well as the location of the supporting testimony and workpapers. The scope of each project is described in workpapers provided in support of this application. Please see the attached testimony and workpapers of Mr. Nichols (SDG&E-18), which were provided in support for the TY2012 request for the WIRED NAC.

C. Please see attachment ORA-SDG&E-DR-036-PM1 Q2 A-C & E-F for a list of the projects as well as the location of the supporting testimony and workpapers. The "intention" of each project is described in workpapers provided in support of this application. Please see the attached testimony and workpapers of Mr. Nichols (SDG&E-18), which were provided in support for the TY2012 request for the WIRED NAC.

D. This is not applicable to the projects listed in response to question 2A above.

E. Copies of Direct Testimony and supporting documents have already been provided in support of this application. Please see attachment ORA-SDG&E-DR-036-PM1 Q2 A-C & E-F for a list of those locations. Please see the attached testimony and workpapers of Mr. Nichols (SDG&E-18), which were provided in support for the TY2012 request for the WIRED NAC.

F. Please see attachment ORA-SDG&E-DR-036-PM1 Q2 A-C & E-F.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

3. Please provide a list of all state and federal cybersecurity mandates SDG&E currently must comply with. Also, identify if SDG&E forecasts new cybersecurity mandates from 2015-2017, if so, provide a list of the possible new state/federal mandates.

SDG&E Response 03:

There are many statutes addressing various aspects of cybersecurity. SDG&E' response is limited to the most relevant cybersecurity requirements, relative to the following:

This response is limited to select cybersecurity requirements relative to the following:

(1) North American Electric Reliability Corporation (NERC);

(2) Federal Energy Regulatory Commission (FERC) and Department of Homeland Security (DHS);

(3) Department of Energy (DOE)—Electric Emergency Incident and Disturbance Report and;

(4) California Public Utilities Commission Decisions;

(5) Cal. Civ. Code Sections 1798.80, 1798.81.5, 1798.82 and 1798.85;

(6) Cal. Bus & Prof. Code Sections 22575-22579; and

(6) Cal. Public Utilities Code Section 8380

NERC

The NERC Reliability Standards CIP-001 (Sabotage Reporting), CIP-008 (Cyber Security-Incident Reporting and Response Planning) and EOP-004 (Disturbance Reporting) impose reporting obligations relative to the physical security, cybersecurity and operational security of the bulk power system. Per these standards, electric utilities must submit these reports within a specified time following the incident or event to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which NERC operates. The "Security Guideline for the Electricity

SDG&E Response 03 Continued:

Sector: Threat and Incident Reporting"[1] describes the relevant event categories and time line for submitting reports to ES-ISAC.

FERC

The NERC reports to the FERC. Currently, the FERC has not established specific reporting obligations for the electric sector relative to cybersecurity; however, it does have regulations in place which treat as confidential Critical Energy Infrastructure Information (CEII) that public utilities submit to the FERC. Essentially, CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (1) relates details about the production, generation, transportation, transmission, or distribution of energy and (2) could be useful to a person in planning an attack on critical infrastructure.[2]

DHS defines CEII more broadly than the FERC to reach "virtual" and "physical" systems. Specifically, DHS defines "Critical infrastructure" broadly as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3]

DOE

DOE requires electric utilities to file an Electric Emergency Incident and Disturbance Report Form OE-417 whenever an electrical incident or disturbance is sufficiently large enough to cross specified reporting thresholds. The DOE uses this information to meet its overall national security and other energy emergency management responsibilities, as well as for analytical purposes.[4]

---

[1] CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE, SECURITY GUIDELINE FOR THE ELECTRICITY SECTOR: THREAT AND INCIDENT REPORTING (NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION) (2008), *available at* http://www.nerc.com/files/Incident-Reporting.pdf

[2] See 18 C. F.R. §388.113(c)(1) and (2).

[3] See Critical Infrastructure Security, http://www.dhs.gov/files/programs/critical.shtm. The DHS has identified critical infrastructure sectors as diverse as food and agriculture, emergency services, transportation and information technology.

[4] See Electric Disturbance Events, http://www.oe.netl.doe.gov/oe417.aspx

SDG&E Response 03 Continued:

CALIFORNIA PUBLIC UTILITY COMMISSION (CPUC)

In D.11-07-056, the CPUC adopted policies to govern access to customer usage data by customers and authorized third parties. In D.14-05-016, the CPUC adopted rules to protect the privacy and security of customer data generated by Smart Meters concerning the usage of electricity provided by the investor owned utilities in California.

California Statutes

Cal. Civ. Code Section 1798.80 requires disposal of customer records no longer needed for business purposes. Cal. Civ. Code Section 1798.81.5 requires organizations to use reasonable security procedures and practices to protect personal information (as defined therein- primarily identity theft sensitive data such as financial account numbers, drivers' license numbers and social security numbers in combination with name elements). Cal. Civ. Code Section 1798.82 generally relates to notification of affected individuals if an organization has reason to believe that their unencrypted computerized personal information (similar but not identical definition to the one in Section 1798.81.5) is breached, but Section (f) thereof also contains a reporting requirement as it requires notification of the California Attorney General if over 500 California residents' personal information is involved. Section 1798.82 also requires 12 months of free credit monitoring for affected individuals if certain identity theft-sensitive categories of personal information are involved. Cal Civ. Code Section 1798.85 governs display, transmission and use of social security numbers. Cal Bus & Prof Code Sections 22575-22579 govern website privacy policies and practices. Cal. Public Utilities Code Section 8380 governs California electric and gas utilities' use and disclosure of customers' energy usage data. These California statutes are all primarily privacy laws not laws enacted for purposes of protecting national security.

SDG&E objects to the second question because it requests speculative information, and thus SDG&E declines to provide a response.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

4. Identify all cyber-attacks on SCG systems in 2013 and 2014. Explain which systems were hacked and the process the hackers used. Also, identify if SCG quantifies the costs to investigate, remediate, mitigate against future attacks, etc. for each attack.

SoCalGas Response 04:

SoCalGas objects to the questions asking that all cyberattacks on SoCalGas systems in 2013 and 2014 be identified and details concerning the hacked system and process be provided because they request information that is confidential because it deals with sensitive information dealing with critical infrastructure, the public disclosure of which could adversely affect the integrity of SoCalGas' operations.

SoCalGas does not currently quantify the costs to investigate, remediate or mitigate against future attacks on a per attack basis.

Without waiving its objections, see the testimony and workpapers of Mr. Christopher Olmsted (SCG-18) for information about SoCalGas' requested revenue requirement for Shared "Information Security".

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

5. Please provide all NERC/FERC compliance reports from 2010-2014. List all violations/possible violations by year, including how SCG remediated the violations/possible violations and mitigation plans for each violation.

SoCalGas Response 05:

NERC requirements do not apply to SoCalGas.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

6. Please identify if SCG has been levied any fines by FERC/NERC, for cybersecurity violations. If the answer is yes, provide yearly fines levied from 2010-2014 (in nominal and test year 2013 dollars).

SoCalGas Response 06:

NERC requirements do not apply to SoCalGas.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

7. Please provide SCG's annual 2012-2014 Review CIP-002 CIP review.

SoCalGas Response 07:

CIP requirements do not apply to SoCalGas.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

8. Please provide a list of each third party SCG contracts with to provide cybersecurity and for each third party provide the following information:
    a. Responsibilities of the contractor.
    b. Responsibilities of SCG to comply with contract terms.
    c. Yearly expenses paid to contractor 2012-2014 and forecast for 2015-2017.
    d. Contract start date and expiration date.

SoCalGas Response 08:

All third party cybersecurity contracts, including their costs originated at SDG&E and were sent over to SoCalGas via shared service allocations. There were no direct third party contracts at SoCalGas.

ORA DATA REQUEST
ORA-SCG-DR-040-PM1
SOCALGAS 2016 GRC – A.14-11-004
SOCALGAS RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

9. Please identify and explain the training materials SCG has used yearly 2010-2014, for cybersecurity training, including the yearly O&M expenses incurred (delineated by labor and non-labor and further by cost center in nominal and test year 2013 dollars) from 2010-2013 for providing cybersecurity training.

SoCalGas Response 09:

All cybersecurity training resources, including their costs originated at SDG&E and were sent over to SoCalGas via shared service allocations. There were no direct costs at SoCalGas for cybersecurity training.

Please see SDG&E's response to ORA-SDGE-DR-036 Q9 for an explanation of the cybersecurity training resources.