ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

Exhibit Reference: SDG&E-19

Subject: IT Cybersecurity

Please provide the following:

1. Please provide SDG&E's policy governing cybersecurity.

SDG&E Response 01:

The SDG&E policy governing cybersecurity is expressed in two documents:

- Information Security Acceptable Use Policy – This policy governs the use of Information and Information Systems (attached as ORA-SDG&E-DR-036-PM1 Q1 Attachment A).

- Information Security Policy – This policy governs the protection of information and information systems (attached as ORA-SDG&E-DR-036-PM1 Q1 Attachment B).

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

2. Please provide a list of each cybersecurity related capital project SCG 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 SCG 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).

SoCalGas Response 2:

A. Please see attachment ORA-SCG-DR-040-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-SCG-DR-040-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 for TY2016 is described in workpapers provided in support of this application. Links to the testimony and supporting workpapers for projects in the TY2016 and TY2012 GRCs have been provided in attachment ORA-SCG-DR-040-PM1 Q2 A-C & E-F. For 2008 testimony and workpapers, please see attachments ORA-SCG-DR-040-PM1 2008 CWP and ORA-SCG-DR-040-PM1 Q2 2008 Testimony.

C. Please see attachment ORA-SCG-DR-040-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 for TY2016 is described in workpapers provided in support of this application. Links to the testimony and supporting workpapers for projects in the TY2010 GRCs have been provided in attachment ORA-SCG-DR-040-PM1 Q2 A-C & E-F. For 2008 testimony and workpapers, please see attachments ORA-SCG-DR-040-PM1 2008 CWP and ORA-SCG-DR-040-PM1 Q2 2008 Testimony.

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

E. Links to the TY2016 and TY2012 Direct Testimony and supporting documents can be found on links listed on attachment ORA-SCG-DR-040-PM1 Q2 A-C & E-F. For 2008 testimony, please see attachments ORA-SCG-DR-040-PM1 2008 CWP and ORA-SCG-DR-040-PM1 Q2 2008 Testimony

F. Please review response on attachment ORA-SCG-DR-040-PM1 Q2 A-C & E-F.

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E 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

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

[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

SDG&E Response 03:-Continued

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]

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

---

[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

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-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

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

SDG&E Response 4:

SDG&E objects to the questions asking that all cyberattacks on SDG&E 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 regarding critical infrastructure, the public disclosure of which could adversely affect the integrity of SDG&E's operations.

SDG&E 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. Stephen Mikovits (SDG&E-19) for information about SDG&E's requested revenue requirement for both Shared and Non-Shared "Information Security".

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E 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 SDG&E remediated the violations/possible violations and mitigation plans for each violation.

SDG&E Response 5:

SDG&E objects to the question as outside the scope of this proceeding because it is irrelevant and immaterial to the revenue requirement requested because SDG&E is not seeking to recover costs associated with NERC/CIP violations in CPUC jurisdictional rates, and is not reasonably calculated to lead to information which would be admissible at hearing. In addition, SDG&E objects to the question as requesting information that is confidential because it deals with sensitive, critical infrastructure information, the public disclosure of which could adversely affect the integrity of SDG&E's operations. Lastly, SDG&E objects to the request concerning "possible violations" as speculative.

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

6. Please identify if SDG&E 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).

SDG&E Response 6:

SDG&E objects to the question as outside the scope of this proceeding because SDG&E is not seeking to recover costs associated with fines levied by FERC/NERC for cybersecurity violations, and is not reasonably calculated to lead to information which would be admissible at hearing. SDG&E also objects to the question as requesting information that is confidential because it deals with sensitive, critical infrastructure information, the public disclosure of which could adversely affect the integrity of SDG&E's operations.

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

7. Please provide SDG&E's annual 2012-2014 Review CIP-002 CIP review.

SDG&E Response 7:

NERC CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment methodology (RBAM). Additional information about CIP-002 can be found at http://www.nerc.com/files/CIP-002-3b.pdf.

SDG&E objects to the question because it is irrelevant to the scope of this proceeding and not reasonably calculated to lead to information which would be admissible at hearing. In addition, SDG&E objects to the question as requesting information that is confidential because it deals with sensitive, critical infrastructure information, the public disclosure of which could adversely affect the integrity of SDG&E's operations.

Without waiving its objections, SDG&E states that its RBAM complies with the requirements of CIP-002. In addition, SDG&E has provided the attached NERC document concerning CIP-002 guidelines.

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

8. Please provide a list of each third party SDG&E contracts with to provide cybersecurity and for each third party provide the following information:
    a. Responsibilities of the contractor.
    b. Responsibilities of SDG&E 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.

SDG&E Response:

Please see attachment ORA-SDGE-DR-036-PM1 Q8.xlsx for Yearly expenses paid to contractors (2012-2014), a forecast for 2015-2016 (item c) and Contract start date and expiration date (item d). Our GRC submission for O&M does not go beyond 2016.

The forecast was pulled together based on information available during the NOI/Application period. In researching the response for this data request, we realized that the supporting documentation contained additional information/costs not reflected in the GRC forecast. The attached forecast includes complete cost information for 2015 (GRC forecast is $563K lower) and 2016 GRC forecast is $953K lower) and therefore does not match the GRC forecast. (ORA-SDGE-DR-036-PM1 Q8.xlsx)

Regarding 8a, the responsibilities of the contractor vary depending on what systems/services provided. Contractors typically provide maintenance updates and support for security solutions. Updates keep security systems current for new threats and patch for vulnerabilities. Some contracts also include services which can include system tuning and optimization. All contractors are bound by negotiated terms (which vary by agreement) and are held accountable to those terms for the life of the agreement.

Regarding 8b, SDG&E's responsibilities vary per agreement. Generally, SDG&E agrees to pay negotiated rates to the contractor. SDG&E intends to uphold its contractual responsibilities.

ORA DATA REQUEST
ORA-SDG&E-DR-036-PM1
SDG&E 2016 GRC – A.14-11-003
SDG&E RESPONSE
DATE RECEIVED: JANUARY 8, 2015
DATE RESPONDED: JANUARY 23, 2015

9. Please identify and explain the training materials SDG&E 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.

SDG&E Response 9:

SDG&E uses a combination of materials for internal cyber security awareness training of company employees and contractors. These include cyber security town-halls, workshops, PowerPoint presentations, email notifications, electronic billboard displays, as well as intranet website articles. These materials are utilized in accordance with a wide variety of regulatory requirements, and industry best practices.

Please see attachment ORA-SDGE-DR-036-PM1 Q9 for the yearly O&M costs from 2010-2013.