Sempra Energy Utilities response Department of Commerce Inquiry on Cyber Security Incentives

APR 29 2013

Sempra Energy's gas and electric utilities collaborate with industry leaders and a wide range of federal agencies on cybersecurity measures. San Diego Gas & Electric (SDG&E) is an owner and operator of infrastructure critical to the reliable operation of the nation's bulk electric system and is thus subject to Department of Energy (DOE), Federal Energy Regulatory Commission (FERC) and North American Electricity Reliability Corporation (NERC) Critical Infrastructure Protection Standards governing the physical integrity and cybersecurity of the bulk power system. Southern California Gas Company (SoCalGas) and SDG&E, as owners and operators of natural gas infrastructure, adhere to best practices and guidelines established by the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and the American Gas Association (AGA) to identify potential SCADA system risks and vulnerabilities and implement prevention and mitigation methods.

Our overall Cybersecurity Program (Program) is a robust system that leverages multiple industry frameworks and standards. The Program is assessed and refined through collaboration with private sector experts and government entities to ensure it meets or exceeds industry expectations. Sempra Energy's practices are based on a risk management methodology that incorporates Department of Defense, National Institute of Standards and Technology and International Organization for Standardization requirements and standards. The initial Program was developed in 2003 and strengthened in 2008 with the Cyber Risk Management approach and strategy. Our methodology supports adhering to compliance objectives, while measuring Program effectiveness using a risk-based methodology to ensure we track and manage risks over time.

The following represents our response to the Department of Commerce Inquiry on Cyber Security Incentives resulting from the Presidential Cybersecurity Executive Order (EO). SDG&E and SoCalGas share the EO's goal of protecting the nation's critical infrastructure from cyber threats and we appreciate the opportunity to respond to this Request and coordinate efforts between the federal government and the private sector.

1. *Are existing incentives adequate to address the current risk environment for your sector/company?*

   We are not aware of any formal incentives for businesses to promote broader adoption of cyber security, excluding potential grants and other research type funding available through the federal government and universities. However, many of the research activities and grants are focused on conceptual work rather than providing tangible products or solution a business can directly benefit from.

2. *Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?*

   Yes. Companies that have access to a larger operating capital invest more and typically have more mature cyber security programs than those of smaller companies. Nevertheless,

companies that have access to larger operating capital still don't have access to sufficient incentives to operate at their lowest possible risk profile. Risk treatment is typically a cost benefit analysis and some cyber security investments can cost more than the resulting impact if the investment was not made. In those situations, companies may typically accept risk and or implement a more cost effective compensating control.

A program should provide incentives for small companies to invest into cyber security programs maturity comparable to companies operating with access to more capital, while incentivizing large companies to do more, so that all companies may operate at the lowest possible risk profile. An industry benchmark should be established by a central oversight and governance organization (preferably a third party audit firm) to develop a standard risk measurement methodology and baseline which is consistent with industry standards as a whole.

Some companies participate in cost and/or time-to-market sensitive markets and have different risk appetites. In these markets, additional incentives can shift the business decision towards making investments.

Finally, any disincentives for disclosing vulnerabilities or cybersecurity incidents should be removed to prevent ignorance from being a more cost effective approach than information sharing and remediation. Inversely, companies that do not promote and or participate in public disclosure can be held liable in situations where an attacker was able to gain access to a vulnerability that was known and not addressed.

Incentives, such as liability protection should be considered for companies that manufacturer or develop systems, software used to provide products and services for critical infrastructure.

3. *How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?*

Business investments are limited and must be balanced between risk management practices and other competing objectives, such as infrastructure, process improvement, social agendas, and others, in order to meet near term and long term revenue goals. In order to make informed business decisions in a complex environment, having access to accurate, reliable information and clear responsibility definitions are instrumental. Our priority is to delivery safe, reliable energy to our customers. A risk based approach is used to determine where benefits may be available. Costs of implementing controls to manage the risks are evaluated by risk owners within the business. The risk owners are accountable for the final risk treatment decision to enhance our cybersecurity.

The two most common methods of assessing risk are quantitative and qualitative analysis. The analysis determines the risk profile which is then treated based on cost versus benefit analysis. Other factors come into consideration, such as whether or not there are any legal requirements,

fines and punitive damages associate to the risk. Where the investment is more costly to the organization than the impact, organizations will typically accept the risk as untreated or apply a compensating control.

A future model should consider a measurement based on risk outcomes versus compliance objectives. Organizations should be measured based on the resulting or residue risk after treatment has been applied (mitigated or accepted).

4. *What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?*

Businesses should be provided financial and or liability protection incentives for operating in a lower risk category. In addition, smaller companies should be offered financial incentives to make more investments into their risk management programs in general.

Liability protection, as an incentive, should be offered to organizations that chose to operate with a lower risk profile than those of industry counterparts. In order for this incentive program to work, the federal government should establish a national benchmark system (operated by a third party such as an audit firm) that establishes the appropriate risk profiles for such incentives. For example, companies operating with low risk could receive liability protection, companies operating with a medium risk, could receive incentives for improvement, such as tax incentives.

Additionally, we feel that accelerated depreciation of cyber security investments would allow for businesses to account for rapid changes in technology to ensure that cyber security protection are able to counter things such as advanced persistent threats.

As it relates to regulated utilities industry, we believe a method to allow for recovery outside of the standard rate structure would ensure that companies are able to react quickly and diligently to real-time and or emerging threats and vulnerability that may have an impact to the reliability and availability of critical infrastructure. On a regular basis, companies have to reprioritize cybersecurity investment to ensure that emerging threats are mitigating or contained appropriately.

Small companies should be incentivized for making security investments to achieve a risk profile that is commensurate with large company maturity consideration and should be given to a maturity phase that is appropriate for smaller companies. A smaller company tends to invest more into manual process controls, whereas a larger company will invest in more technology to automate process to streamline operations, reduce cost and complexity while improving

visibility. In either case, a risk profile should be consistent yet consider the size of the company and how investments are made over time as the company matures.

Specific ways to encourage businesses are:

- Timely, actionable threat information for the risk owner's decision making processes,
- Access to threat and vulnerability intelligence,
- Certification processes for vendors or partners that provide critical infrastructure personnel, products, and services,
- Liability protections for businesses participating in industry accepted risk management programs,
- Market and financial incentives for cybersecurity research, products and services,
- Accelerated depreciation of assets related to technology, and
- Incentives for replacement of antiquated technology used for the protection of critical infrastructure.

5. *How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?*

   Success or failure is based on the measurement of control (process or technical) requirements and standards ability to effectively manage risk. If a control is deficient or operating incorrectly, that control is measured for its impact to a risk area. A control gap is treated as deficiency. Cost effectiveness is an assessment that is made before risk treatment to determine if the cost of the control is less than the impact or liabilities related to a risk outcome. A company risk profile can be measured across the industry based on how others perceived risk outcomes. Currently there is not an industry standard measurement for companies to refer to. A company's risk profile should be measured against the industry to determine if the resulting risk or risk outcome aligns with what was determined by the industry given similar standards and requirements.

   Success is based on real and estimated potential losses versus costs. Incident actuary information from an insurance or liability protection organization could further quantify the effectiveness and value of risk management programs.

6. *Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?*

No, we have not seen incentives that promote better security practices and most of the incentive based on fines and punitive damages has only been effective in promoting a culture of compliance (satisfying the letter of the law) as opposed to increasing the effectiveness of cyber security programs and controls. Most of the compliance legislation is created with good intentions but those programs become stagnant over time and ineffective in dealing with rapid changes in technology.

Indirect incentives to encourage proactive investments and practices, such as ES-ISAC and NIST standards development, have been helpful.

Additional risk mitigation, market enablement, and financial incentives would enhance the allure of security investments.

7. *Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?*

The first disincentive is the cost of implementing a program and the cost of purchasing and implementing controls (process and technical) to manage risk effectively. Smaller businesses are disadvantage in that they do not have access to the capital necessary to make more prudent cybersecurity investments or hire expensive skilled staff. In order to minimize the disincentive for small businesses, tax incentives or rebates should be offered for cybersecurity investments in personnel and technology.

Inconsistent multinational laws and regulations make it difficult to standardize approaches which are counterproductive to company growth. To ensure products and services meet cybersecurity requirements, a multinational program and certification authority should be established to develop multination standards, a system of measurement and certification which can then be leveraged to review and approve potential products and services. To keep small business's offerings competitive, stipends based on their resources could be offered to offset any certification costs.

Risk exposure is consistent amongst small are large business but the impacts may differ. Although small businesses are exposed to the same risks as larger organizations, they can be more cost sensitive due to available capital for investments and a business focus on growth as opposed to a balance between stability and growth.

8. *Are incentives different for small businesses? If so, how?*

We are not aware of any incentives that exist for small businesses. However, there are legal and regulatory mandates that apply equally to small and large businesses. Under such a legal and regulatory landscape, it is likely that smaller businesses will not make the necessary investment to minimize risk beyond what is an acceptable cost/benefit outcome. (Meaning that many small businesses will look at the cost benefit analysis and if the cost of the penalty/fine or loss of market opportunity is less than the cost of implementing what is required by the regulatory/legal scheme, they will opt to take the penalty, as the lower cost option).

We do not qualify as a small business; however we try to dedicate a portion of our outsourced budget to disadvantaged businesses. In general, their success is sensitive to the additional overhead of addressing financial and resource impacts related to cybersecurity. Tax incentives provided to larger companies would provide incentives to work with smaller suppliers to improve the risk posture of their products and services.

9. *For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?*

Yes. The cost of managing a compliance program is typically very high (8-10% of costs) and burdensome to business, because compliance programs fail to adequately address cyber security and privacy issues and focus more on appearance as opposed to practice. Therefore, businesses typically have to make additional investments into cyber security to have a robust program that is able to adequately deal with cyber security threats and vulnerabilities.

Additionally, mature companies make additional investments (additional 5%-20%) into cybersecurity programs beyond what is required by regulations and laws.

10. *What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?*

First, we do not agree that holding an organization accountable for failure to exercise reasonable care should be called an incentive but rather a penalty

We believe that companies should be afforded legal-safe harbors for participating in a voluntary sharing scheme under the DHS program, with an exception for instances where a company

engages in illegal behavior or gross negligence that has an impact on national security or results in loss of life.

Safe-harbor incentives should require participation in information sharing program and a standardized multinational risk management program. The benefits should include liability protections or limits based on resulting risk outcomes of treated or untreated risk. Participation in such a program should shield participants from fines, penalties and punitive damages due to transparency into an organization's risk management process.

11. *What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors?*

    The beneficial impacts would be an establishment of a baseline level of risk practices, better identification of the industry participants, improved information available for decision making, common cybersecurity practices, and the potential for more effective incident response.

    The negative impact would be additional costs of products and services which could be offset by assistance after joining the DHS Program.

12. *How can liability structures and insurance, respectively, be used as incentives?*

    If an organization has a risk management structure, at some point the costs associated with managing a given risk is prohibitive. A liability structure addresses this situation by:

    - Pooling expensive risk mitigation solutions to provide an opportunity for a larger organization to either mitigate or absorb the impact
    - Limits liability exposure in situations where a control has been applied in a standard way, been reviewed and found compliant, and fails for some reason
    - Requires participants to perform a thorough risk analysis in order to determine what risks can be managed within the business and those that require external management

    Additionally, actuary information for informed risk management could be collected as the liability structures and insurance constructs are applied to incidents.

13. *What other market tools are available to encourage cybersecurity best practices?*

    Certification of products and services provided by third parties and background checks for personnel in positions with cybersecurity impacts are two tools that have been applied in some industries. Security clearances sponsored by DHS or another suitable government department

could be used to manage the flow of threat information to business decision makers to facilitate informed risk management.

In the utility industry, recovery of cybersecurity costs within the utility and in support of its suppliers via federal rate applications would address the nature of critical infrastructure impacts due to cybersecurity incidents. The cost areas could be determined by best practices as determined with the DHS Program.

14. *Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?*

    Yes, a singular effort to develop an effective risk management framework would greatly improve the effectiveness and efficiency of business and promote a broader adoption by the industry and potentially the world. By giving business the freedom to determine the best treatment option based on a menu of standards and requirements (controls), the business would be able to adapt to a changing environment as necessary, reduce complexity with multinational trade. An industry consortium or standards body can be established (US and Abroad) to administer and manage certification and measurement, while local incentives can be developed to promote adoption at the local and federal levels.

    A clearance program should be extended to the critical infrastructure businesses. Sensitive threat information could then be shared with key business decision makers within critical infrastructure areas in support of the risk management and incident response processes.

15. *In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?*

    Tax incentives for businesses purchasing products and services from small businesses and multinationals could be used to drive implementation of the risk management guidance and standardize a system which measures organization based on risk outcomes. The current challenge is that compliance objectives are to focused and do not lend well to multi-national disciplines because of the focused objectives. If measurement was based on risk outcomes, then businesses would be given more flexibility to adapt to different standards and controls and achieve the same outcome.

16. *What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?*

    We are not aware of any incentives that drive changes in standards and best practices once adopted other than reactionary changes which have a tendency to follow main-stream attention as opposed to being proactive in dealing with threats and vulnerabilities.

    Maintaining risk management controls can be maintained by:

    - Periodically recurring compliance requirements
    - Specifying vulnerability testing and patching requirements
    - Providing updated threat intelligence
    - Structuring risk management so that it can be updated quickly as risks and threats change by defining standard formats or by hosting the business specific risk assessment analysis within the DHS Program.

17. *Voluntary industry sector governance mechanisms are sometimes used to stimulate organizations to conform to a set of principles, guidelines, and operations based on best practices, standards, and conformity assessment processes that collectively increase the level of assurance while preserving organizations' brand standing and the integrity of products and services.*

- *Do organizations participate in voluntary governance mechanisms?*

  Sometimes, if it is beneficial and cost effective, overall. It cannot be perceived to add additional risks, such as exposed intellectual property or sensitive business plans.

- *Which industries/groups have voluntary governance mechanisms?*

  NIST, ISO 27000 Series, and many other industry workgroup efforts.

- *Do existing voluntary governance mechanisms have cybersecurity-related constraints?*

  Yes.

- *What are the benefits and challenges associated with voluntary governance mechanisms?*

  Under a voluntary mechanism, commitment may be temporary so a false sense of security may arise and voluntary mechanism's tend to lack sufficient oversight to provide broader industry value because they tend to focus on a particular industry segment which makes the

implementation and ongoing maintenance complex The benefit is that a particular industry segment may be more likely to adopt those standards but that in itself also causes issues because many of those industry standards do not extend to other industry segments very well and results in exclusion or division of industry standards.

SDG&E and SoCalGas appreciate the significance of this issue, and we welcome the Department's leadership and continued focus on cybersecurity policy. Should you have any questions or need any additional information, please contact either Jeffery Nichols, Director, Information Security and Information Management, JCNichols@semprautilities.com, 858-613-3216 or Scott King, Information Security Manager, SKing@semprautilities.com, 858-613-5718.