Sempra Energy utilities response NIST RFI - Experience with the Framework for Improving Critical Infrastructure Cybersecurity

October 9, 2014

Sempra Energy's US-based gas and electric utilities, San Diego Gas and Electric (SDG&E) and Southern California Gas Company (SoCalGas), collaborate with industry leaders and a wide range of federal agencies on cybersecurity measures. 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 electric system.

As owners and operators of natural gas infrastructure, SDG&E and SoCalGas 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), covering both SDG&E and SoCalGas, 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 that it meets or exceeds industry expectations. SDG&E and SoCalGas' practices are based on a risk management methodology that incorporates Department of Defense, National Institute of Standards and Technology (NIST) 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.

SDG&E and SoCalGas appreciate the opportunity to provide information regarding how we protect our electric grid and natural gas assets from cyber-attacks. SDG&E and SoCalGas encourage continued coordination efforts by NIST among the federal, state, local government, and the private sector to ensure the security of the nation's energy systems.

NIST Cybersecurity Framework RFI Questions (add additional feedback at the end of the appropriate section)

<u>Current Awareness of the Cybersecurity Framework</u>
Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

> Within the energy industry, much of the awareness has been focused on the Department of Energy (DOE) Guideline development effort and the Cybersecurity Capability Maturity Model

(C2M2) tools (Electric Sector and Oil and Natural Gas). Sempra Energy's gas and electric utilities, Southern California Gas Company (SoCal Gas) and San Diego Gas & Electric (SDG&E) have done initial assessments and have found the results informative. There is ongoing work to map the C2M2 assessment results back to the NIST Cybersecurity Framework (CSF) using a draft of the Guideline.

In addition to internal use of the tools, SDG&E and SoCalGas have participated in industry group discussions to develop a common understanding of the application of the assessments.

In the first six months since the release of the Framework, it has influenced how SDG&E and SoCalGas manage cyber risks. Our evaluation is continuing as the DOE Guidelines and other elements of the overall program complete their development. Because SDG&E and SoCalGas are already held to more stringent standards elsewhere, we will consider implementing parts of the framework that align with internal strategies, policies, goals and requirements. The degree of adoption could also be influenced by additional incentives that have yet to be defined.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

SDG&E and SoCalGas learned about the framework through multiple sources: direct outreach from NIST, interaction with company representatives in Washington DC, and through several industry groups that we are either members of or participate in. SDG&E and SoCalGas have participated in the framework efforts since inception, via commenting on the initial Framework Request for Information as well as the workshops held during the drafting phases.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

Yes, SDG&E and SoCalGas are working with sector-specific groups to receive and share information.

4. Is there general awareness that the Framework:

a. Is intended for voluntary use?

Yes. This message has been consistently reinforced.

b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

There is a general awareness within the organization about the Framework. The ultimate efficacy of the framework for SDG&E and SoCalGas is currently under evaluation. The results of the evaluation by the subject domain experts will determine the Framework's utility within the organization.

c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

There is an awareness that the framework is built on existing tools. There is also awareness that it provides flexibility in the use of other tools for specific practices.

5. What are the greatest challenges and opportunities – for NIST, the Federal government more broadly, and the private sector – to improve awareness of the Framework?

The greatest challenge is for the Framework to demonstrate additional benefits beyond similar frameworks and tools already in use. As the program currently stands, adoption of the Framework is driven by the benefits versus the costs of program changes. Specification of incentives to adopt the Framework may change the benefits and accelerate integration of the Framework into the industry.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

SDG&E and SoCalGas' focus has been on domestic use of the Framework. We are not aware of the international awareness level of the framework.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

Regulators are aware of the Framework and have been involved in its evolution.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

SDG&E and SoCalGas participate in external education of cybersecurity risk management within our community, industry, and suppliers. We also have a robust internal cybersecurity outreach and education program. However, at this point, the outreach has not included awareness of the Framework. In the future, SDG&E and SoCalGas anticipate supporting such outreach programs that specifically address the Framework with other entities, such as DHS. For example, SDG&E is assisting in the coordination of the C3 Voluntary Program in San Diego in October 2014.

9. What more can and should be done to raise awareness?

Once the Framework and related tools within critical infrastructure industries are more mature, awareness activities will be more effective. Currently, the focus is on the internal use and application of the Framework. When this activity has progressed, an awareness campaign will have specific services available.

Experiences with the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

1. Has the Framework helped organizations understand the importance of managing cyber risk?

SDG&E and SoCalGas have had a robust cyber risk management program in place for many years. The Framework has had a positive effect on our organization and has helped reiterate the importance of cyber risk management. The assessment process acts as an effective awareness tool.

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?

SDG&E and SoCalGas' critical infrastructure sectors are the electric and natural gas sectors. These sectors are actively planning and some cases using the Framework. So far, the bulk of the activity has centered on the DOE ES-C2M2, ONG-C2M2, and C2M2 tools. The activity includes pilot testing, active use, and industry base lining.

3. What benefits have been realized by early experiences with the Framework?

Early experiences have included identification of areas for program enhancement and increased awareness of cybersecurity risks.

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

The assessment tools have provided a mechanism to improve reproducibility, enable best practices discussions, and raised the general awareness and urgency of addressing cybersecurity risks.

Additional effort on aligning risk management objectives and acceptable levels of risk are required. There is not a method to appropriately manage risk across all stakeholders.

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

The Electric and Natural Gas sectors do not need additional control guidance beyond what is currently under development.

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

That effort is currently underway within our organization.

7. Is the Framework's approach of major components – Core, Profile, and Implementation Tiers – reasonable and helpful?

Yes.

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.

a. Of these recommended practices, how are organizations initially using the Framework?

SDG&E and SoCalGas are primarily using the Framework to improve our cybersecurity program (3.2).

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

The Framework can also be used exchange best practices within an organization or industry. After an assessment, differing maturity levels can indicate areas where exchanging ideas may be most beneficial.

c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

SDG&E and SoCalGas maintain an Office of Customer Privacy (OCP) tasked with enabling and advocating for customer privacy both internally, as well as externally. The OCP uses Privacy by Design as guiding principles in order to ensure new projects, including cybersecurity-driven projects, are protecting customer privacy following an industry-recognized set of privacy controls known as the Generally Accepted Privacy Principles (GAPP). These principles are similar in nature to the ones described in section 3.5 of the Framework. The OCPs manage a set of privacy controls based on state and federal regulations that meet or exceed what is recommended in the Framework. In cases of breach detection and response, generally, security incidents involving authorized third parties, such as law enforcement, do not typically include customer data elements that can be used to identify an individual customer. However, in the rare cases that do involve specific customer data elements, the Information Security team works with the OCPs and our Legal departments to ensure that the protection of customer privacy is being considered and respected at the same time the incident is being handled in a timely fashion.

d. Are organizations changing their cybersecurity governance as a result of the Framework?

Our organization is not changing our cybersecurity governance as a result of the Framework. We are applying it as an additional tool to improve our program.

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs – including the effectiveness of those programs – to stakeholders, including boards, investors, auditors, and insurers?

Not yet, though that seems a likely outcome. This area requires additional development of methods and incentives before it can be used to align perception and management of risk among stakeholders. It would be beneficial if additional focus was placed on developing a coordinated risk management policy framework. In general both the government and industry understand how to identify and manage risk; the gap is more one of aligning the disparate risk management policies.

For example, if the government stakeholders (USA, Canada, and Mexico) defined their risk profiles, or something similar, and industrial entities did the same, then the gaps in the risk expectations could be identified. In addition to the risk profile alignment, the guideline could also provide a description of the risks that should be considered in order to ensure that each industrial entity addresses the relevant risk scenarios. Finally, the government stakeholders could prioritize their profile to emphasize where they perceive the greatest impacts. The incentives discussion would then be part of addressing gaps between risk decisions based on a prioritized set of public expectations versus business-oriented risk decisions. The discussion could be tailored based on the entity's industry, market impact, and national infrastructure served by the entity. Essentially, the framework should identify risk-oriented use cases of value to the public beyond those currently addressed by industry best practices and the incentives to motivate their implementation.

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

To date, SDG&E and SoCalGas use internally developed approaches that align with those described in the framework.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

No comment.

10. Have organizations developed practices to assist in use of the Framework?

SDG&E and SoCalGas are currently integrating the Framework into our cybersecurity program. The DOE Guideline for using the NIST CSF has developed practices which will be helpful. It also includes security control mappings to the NIST CSF as well as other accepted standards, such as NIST SP 800-53 and NERC CIP.

Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?

The Roadmap identifies the key areas.

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

Consider enhancing section 4.2 "Automated Indicator Sharing" to include tools and best practices for indicator management. Organizations are faced with managing large numbers of technical indicators that have varying life spans, different degrees of quality/confidence, and include varying amounts of contextual information. We need tools and processes to manage the operational lifetime of indicators (when should an indicator be removed from a preventive control?), manage deployment of indicators based on source reliability, and relate indicators based on additional contextual information.

3. Have there been significant developments – in the United States or elsewhere – in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?

No comment.

SDG&E and SoCalGas appreciate the opportunity to respond to this RFI, and we welcome NIST's leadership and continued focus on cybersecurity. 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.