SDGE®

Southern
California
Gas Company®

Sempra Energy® utilities

Sempra Energy Utilities Response NIST Preliminary Cybersecurity Framework Comments

13 DEC 2013

SDGE Southern California Gas Company
Sempra Energy utilities

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 NIST Cybersecurity Preliminary Framework developed as the result of 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. NIST poses the following questions in the Preliminary Framework:

Does the Preliminary Framework adequately define outcomes that strengthen cyber security and support business objectives?

Additional guidance o a common prioritization methodology should be added to the Framework. The controls within the framework core appear to be equally important but probably are not as they mitigate different risks or have a higher priority for sensitive systems. In addition, information o how to develop a target profile for a business and then how to map the profile to specific business processes or systems would also be helpful.

Does the Preliminary Framework enable cost-effective implementation?

Cost effective implementation is depended upo appropriate incentives.

Does the Preliminary Framework appropriately integrate cyber security risk into business risk?

The framework should include some kind of guidance about appropriate levels of investment in security controls, including proposing an adaptable way for an enterprise to calculate appropriate investments given the conditions in their environment.

Does the Preliminary Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?

There doesn't appear to be common gauge of risks and the value of mitigation of risk impacts that can be used across industries to meet national objectives in resilience. Directors from multiple industries should be able to compare risks in general critical infrastructure risk areas. For example, common risk reporting formats, terminology, and metrics. These tools would provide the basis for communicating cyber risks between multiple stakeholder groups as well. In addition, to provide additional motivation to invest in mitigating cyber risks, the Framework should provide implementation timeline objectives which are tied to incentives and voluntary participation.

Does the Preliminary Framework provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?

Additional guidance o how to develop target profiles should be provided. The guidance should take into account the industry, regional features (such as military installations, national industry hubs, and other critical infrastructure organizations in the area) to work towards regional resilience.

Does the Preliminary Framework provide the right level of specificity and guidance for mitigating the impact of cyber security measures on privacy and civil liberties?

Standardized risk scoring and risk taxonomies for privacy/civil liberty impacts across infrastructure industries should be included with cybersecurity risk scoring.

Does the Preliminary Framework express existing practices in a manner that allows for effective use?

The framework could improve existing practices by proposing reproducible evaluation scoring framework that could be compared across industries and organizations. Additionally, independent, accredited assessors could leverage such scoring system to provide consistent metrics. Some level of confidential transparency into current posture and progress reaching target postures is necessary to gauge at critical infrastructure level whether industries and organizations are leaders, adequate performers, or weak links.

Will the Preliminary Framework, as presented be inclusive of, and not disruptive to, effective cyber security practices in use today, including widely-used voluntary consensus standards that are not yet final?

The framework is as usable as any other framework and doesn't seem to propose any new standards. It may be less disruptive and more cost effective to require adherence to NIST 800-53 and 800-82, and provide specific guidance about what characteristics or conditions drive classification of assets as high/medium/low for ICS security purposes.

Will the Preliminary Framework, as presented enable organizations to incorporate threat information?

risk taxonomy included directly or by reference in the instructions for "Step 3: Conduct a Risk Assessment" (line 417) would be helpful to avoid overlooking potential risk areas during the assessment process. There should be some criteria for linking open-source intelligence about threats and vulnerabilities to ICS customer knowledge about their own systems. For example, "Events A and B are being reported in the news, I know that I have product and that is vulnerable to and B, therefore the threat level is medium."

Is the Preliminary Framework presented at the right level of specificity?

The security framework should extend to the commercial space, where specific criteria are adopted for ICS equipment and software that are considered ICS-Safe. This would encourage or drive the adoption of some kind of certification scheme where the following objectives are met:

- ICS hardware, software, and systems must not be dependent on equipment, software, or systems that are no longer supported by the vendor.

- ICS hardware and software must ensure that components or libraries from third party vendors are supported by an effective vulnerability management program, and updates for known vulnerabilities are provided to customers as they become available.

- Vendors and support organizations must not require activity by ICS customers that is considered detrimental to the customer's security. (e.g. requiring back doors, requiring the use of unsupported libraries or operating systems, forcing the use of insecure communication protocols, etc.)

- ICS vendors and service providers who place restrictions on customer architecture, controls, or communication should be held directly accountable by regulators for regulatory violations, and should be subjected to the same penalty structure as the customer.

- The framework should include workflow for determining and assigning responsibility of control owners (whether that's the vendor, the integrator, pro services organization, or the ICS customer) and should include the responsibility assignment with the controls that are required. (e.g. Vendor must provide patches. Customer must patch.)

- Some method of grading and addressing variances to the control framework should exist. For example, utility or product that meets all the criteria should be considered compliant. A vendor that sells unsupported or partially supported equipment (for whatever reason) should be considered degraded. A integrator that fails its audit should be uncertified.

- The framework should include criteria for appropriate architecture with specific guidance for achieving required service levels. For example, utility should not be designing in single points of failure for critical infrastructure, nor should vendors be building products that rely on unreasonable conditions (like "we want to remotely manage the system for you" and at the same time "something this important should be in an isolated network.")

Is the Preliminary Framework sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

methodology for assessing risk trade-offs between privacy/civil liberties and cyber security controls within the Framework Core would be helpful.

Other Suggestions

In section 2.4, Framework Implementation Tiers, a recommendation to evaluate the organization's effectiveness for each tier and area using proposed scoring methodology would help businesses identify inconsistent and/or partially implemented practices.

Conclusion

SDG&E and SoCalGas appreciate the significance of this issue, and we welcome the agency's leadership and continued focus on cybersecurity policy. We look forward to working with the Taskforce on this important topic. 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, Manger of Information Security, SKing@semprautilities.com, 858-613-5718.