Sempra Energy Utilities response NIST RFI - Cyber Security Framework

APR 08 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 NIST Request for Information for the purpose of developing a cybersecurity framework 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. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

We view the following as the greatest challenges in improving cybersecurity practices across critical infrastructure. First, the lack of a developed and enforceable common set of broad security practices that vendors and third parties must adhere to when providing critical infrastructure products and services poses the most significant challenge to organizations. Second, when procuring goods and services from foreign countries, organizations are challenged by the absence of strong controls on supply chain commerce. Third, the inability to utilize federal government capabilities for background investigations of employees operating in sensitive roles presents additional challenges for employers. Finally, the lack of a risk management and compliance framework that assesses based on risk outcomes versus compliance mandates and objectives causes challenges as well.

It is our belief that compliance should be viewed as a process control that is designed to identify control weaknesses as opposed to a means by which individuals and/or organizations are penalized. Current compliance practices fail to incentivize the identification of failures or gaps which may lead to organizational ineffectiveness when critical issues are typically not reported. An additional challenge is partnering with the vendors of critical infrastructure to develop and design upgrade paths for better securing the industrial control systems themselves.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

If enforceable uniform standards are developed and applied nationally, and the measurement and enforcement of those standards (controls) is based on a risk outcome versus compliance objectives (control standard enforcement), then we see few or no challenges in developing a cross-sector standards based Framework. Organizations should be able to choose the most effective control based on the situation and/or intelligence. Measurement should occur at a risk level whereby controls are aggregated to produce an overall risk picture. Control standards should allow an organization to choose from a set of controls. An incentive model (liability protection) should be adopted for organizations operating at an overall lower risk than the industry average.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

The Enterprise Risk Management (ERM) policy, posted on company’s Intranet, establishes the guiding principles for managing the key risks. It defines roles, responsibilities and processes for the ERM activities. The oversight responsibility for all risk management activity resides with the Board of Directors. The ERM Committee, consists of 10 officers and meets quarterly, is in charge of ensuring the company has a holistic approach in its risk assessment and treatment, is vigilant in risk mitigation and is prudent in resource allocation and capital investment. The ERM framework is supported by the Risk Management Department in conjunction with a multi-disciplinary ERM Advisory Council.

The information security risk and compliance programs within our company are supported by policies that span across the organizations. The enforcement occurs through the development and implementation of a complete risk management program. Controls are developed, implemented and related to assets. Assets are then associated to information which is then related to an area of risk. As a control fails, it impacts the risk posture of one or more areas of risk. Process controls operate within their own unique set of requirements.

4. Where do organizations locate their cybersecurity risk management program/office?

SDG&E and SoCal Gas' cybersecurity risk management program is located within an Information Security department reporting directly to the company Chief Information Officer.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

Risk may be defined as the exposure to uncertainty which may prevent the attainment of objectives. Risk is typically assessed based on the combination of the strength (effectiveness) of existing controls; the likelihood, within a period of time, of a risk event occurring; and the severity or impact, of the event. Severity may be determined by the health and safety impacts to employees and customers, the disruption to company operations which could affect customers, or the financial impact.

Cybersecurity risks are defined as threats to information and technology assets that affect the confidentiality, availability and/or integrity of the information and information systems and have a negative impact to company operations or finances. In addition, most cybersecurity risks are typically defined based on a financial threshold, where the organization cannot tolerate a loss. Some organizations, including utilities, have also identified some events or outcomes that are intolerable regardless of the financial impact and design controls to prevent them. Risks are assessed based on measurement of the effectiveness of controls (standards) designed to manage that risk. If the controls operate as expected and as designed, risk posture is reflective of the risk outcome achieved by the introduction of that control. Control gaps and deficiencies are measured as failures. For instances where a control cannot be implemented, a compensation control is used in addition to the risk owner accepting risk for a high risk situation.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Cybersecurity has been identified as a key risk of the organization within the existing ERM framework. Cybersecurity risk owners and managers have the authority and responsibility for identifying, measuring, and managing cybersecurity risks and threats in addition to implementing effective risk mitigation and contingency plans.

Cybersecurity is an area of risk whereby specific security controls are developed based on industry standards and requirements. The security controls are a subset of other business controls designed to manage risk across the organization. Risk measurement is achieved through the measurement of control operation (Gaps and Failures). Controls are managed by control owners and control subject matter experts. Updates on cybersecurity risk and mitigation are periodically reported to the Enterprise Risk Management Committee.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Our organization has adopted best practices and requirements from numerous industry sources, such as NIST, ISO, IEEE, FERC, NERC, DoD, DHS. Numerous industry experts were consulted to develop the risk management framework because a complete industry framework that defines an end to end risk management lifecycle did not exist. Our organization has leveraged process and workflow automation technology that can manage process controls as well as the measurement of technical controls related to areas of risk and their respective owners. In addition, process controls are being used for many of the cybersecurity elements, such as incident response and vulnerability management. The process controls leverage both industry standard elements as well as internally develop methodologies.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

This is a complex question because "under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure." [1] Moreover, there are more than 50 statutes addressing various aspects of cybersecurity.[2]

This response is limited to select cybersecurity regulatory reporting 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 (CPUC) Decision (D) 11-07-056 (Smart Meters Privacy Decision); and

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

NERC

[1] For a comprehensive overview of this topic, see ERIC A. FISCHER, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS (Congressional Research Service) (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42114.pdf

[2] *Id.*

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"[3] 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.[4]

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."[5]

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.[6]

CALIFORNIA PUBLIC UTILITY COMMISSION (CPUC)

[3] 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

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

[5] 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.

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

In its Privacy Decision[7], 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. In addition to protecting the privacy and security of usage data, the Privacy Decision also adopts policies to govern access to customer usage data by customers and authorized third parties.

Cal. Civ. Code 1798.80, 1798.81.5 and 1798.82

Cal Civ. Code 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 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 regulatory reporting requirement as it requires notification of the California Attorney General if over 500 California residents' personal information is involved. These California Civil Code statutes are all primarily privacy laws, not laws enacted for purposes of protecting national security.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Our company is an owner and operator of significant critical electric transmission facilities that are part of the interconnected western grid of the United States, Mexico and Canada, as well as critical natural gas transmission facilities. This grid is interconnected and interdependent with the transmission grids of utilities across the western interconnect. While current transmission planning seeks to ensure that the bulk electric system can sustain the loss of its largest single contingency, a major disruption would be difficult for the system to absorb without some loss of reliability.

This transmission system also relies upon a myriad of electricity generation facilities located throughout the region. Planning ensures that the system can withstand both planned and unplanned outages of generation; widespread outages combined with high levels of demand can, and sometimes do, result in the loss of the ability to deliver power to all customers. In such a situation the grid sheds load (limited blackouts) in order to prevent more widespread outages.

[7] Decision 11-07-056, *available at* http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/140369.pdf

The electric generation that we rely upon to meet the demands of our customers is provided by independent power producers as well as our own generation assets. These generators are dependent on a reliable natural gas system. The electric generation in our region relies upon the local distribution system, the interstate gas transmission system and in-region gas storage to reliably provide the natural gas required to meet their demands. While we see an increasing role of renewable generation in our region, and in across the nation as a whole, system reliability is maintained by natural gas plants. The reliability of the generation fleet is dependent on a reliable flow of natural gas.

Our largest electric generation facility is dependent on a local water distribution system in order to continue generating. We rely upon our own telecommunications infrastructure as well as public telecommunications infrastructure to effectively operate our business. If the reliable service of these services is disrupted significantly it could result in serious reliability issues for the electricity grid. In California, the California Independent System Operator relies on the telecommunications infrastructure to dispatch electric generation required to meet the demands of the systems.

Our company, like the rest of the electricity market, is highly dependent on a functional market for electricity to procure the power needed to meet demand. This market for electricity relies upon the liquidity and functioning of financial markets in order to function properly. A significant disruption of the nation’s financial markets and the confidence that participants have in that market can lead to disruptions in the market for electricity as well.   If parties are unwilling or unable to trade because of a disruption in the financial markets, the reliability of the electricity grid would be threatened.

To meet the challenges of a reliable flow of natural gas, our natural gas transmission pipeline system serving the regional generating fleet, and nearly all natural gas end-use in our region, is designed to continue to operate without utility electrical power for significant periods of time. This attribute serves the restoration of electric generation in the event of a major disruption in either out-of area generation or companion electric transmission lines serving our area. Our company’s gas transmission systems employ several tactical approaches to achieve this service security, including on-site natural gas-fired electric generation to restart and operate major compression and gas-handling facilities, back-up battery power (uninterruptible power supplies), portable generators and dispatch of personnel to place assets in mechanical override, where applicable. Testing of these systems and processes is also integral to our operational planning.

Our company also leverages the storage of gas in underground geological formations and makes full-use of gas stored in pipelines to contend with disruption in supplies from out-of state pipelines and/or when key pipelines within its transmission system are out-of-service. This storage of energy constitutes a fundamental difference between natural gas and electric energy management and delivery. The company fully leverages this physical characteristic to support electric grid reliability/restoration.

Our company performs remote central monitoring through a central gas control operation which is dependent on private telecommunications. We are utilizing the FCC administered Telecommunication Service Priority program, in order to facilitate rapid restoration of control and monitoring telemetry circuits during and after natural or technical disasters.

National Security

Many national security assets rely upon the electric grid to perform their critical functions. Back-up power may allow certain highly critical functions to continue, a sustained electric outage could undermine the efficacy of their operations with a potential degradation of these assets' performance. In our region, there are numerous naval and marine bases and operations. Additionally there are significant Homeland Security facilities and operations in the area. Maintaining reliable power for these critical functions is a high priority for our organization.

Health and Safety

The region's emergency response and management is also highly dependent on a reliable, robust and resilient electricity infrastructure. Police and fire operations are dependent on electric service. Hospitals and other emergency medical facilities have some ability to continue limited operations in the case of an outage, the long-term sustainability of these operations are hindered by the lack of grid based power.

Many individual customers have health issues and rely upon electric devices to maintain their health (e.g., oxygen machines, life support systems). Electric outages for these customers can be, and often are, life threatening events. In addition, during certain times of the year in parts of our county, people may face triple digit heat. Lack of cooling caused by a disruption in the electricity system may negatively affect segments of the population.

Economy

Nearly every sector of the economy is dependent on a reliable electric grid. Below are a few of the key sectors that would be directly impacted by events that impacted the national electricity grid.

- Water: The region's water infrastructure relies upon electricity for pumping and treating water. While some facilities have back-up generation, this is not universally the case and in many instances such back-up generation cannot be sustained over a longer period of time. Sewage treatment facilities are also dependent on electricity for their reliable and safe operations.

- Telecommunications: Telecommunication providers require reliable electrical power to ensure the sustainable operation of the networks that make up today's telecommunications sector. While many facilities have back-up power of some sort, this often cannot be sustained indefinitely. As customers have begun to rely more heavily upon internet telephony, they have also become more dependent on electricity being delivered to their house because internet based telephony requires an independent source of power rather than using power provided by the network itself as was the case with the traditional public switched network. The proliferation and increased dependence on wireless communication also requires both the wireless carriers' antenna and individual handsets to have reliable sources of power in order to function.

- Transportation: Air travel is also highly dependent on a reliable electricity grid. Air traffic control requires electric service to maintain its operations, and at night runways and taxi-ways require electricity for their required lighting. Within a city, traffic can be bought to a halt as loss of power causes traffic lights to fail and light rail that relies upon electricity for power is brought to a halt. Though our area has no refineries, the national oil refineries rely on a dependable source of power to keep the nation's supply of gasoline and diesel fuel flowing so our nation's trains, trucks and automobiles can stay on the road.

- Information Technology: The information technology sector relies upon reliable power in order to keep functioning. While many companies and organizations that rely upon information technologies have back-up power and other contingencies in place, electric power outages can and do disrupt the operations of information technology.

- Banking: Banking is increasingly electronic in nature. Many consumers rely on the use of debit card and credit cards for their transactions rather than cash. Customers rely upon ATMs for their sources of cash, sources that rely upon electricity to function. Bank branches rely upon electronics to track transactions and to ensure that funds withdrawn are actually on deposit.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Performance goals start at the organizational level with the definition of a corporate strategy which is propagated down to the individual contributor level. Goals and objectives are used to ensure compliance activities are managed as expected by control owners and subject matter experts that have the responsibility for the implementation and maintenance of controls. Compliance controls are mapped to risk areas that are managed by risk owners and managers. Key performance indicators and goals are established to ensure that risk outcomes are appropriately managed. Overall corporate goals are managed at the risk committee level where risk performance is measured for effectiveness.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Our organization has adopted an approach that complies with legal requirements and reflects an industry standard approach to reporting. Additionally, we have established reporting relationships with local and federal law enforcement entities. We report issues such as the following:

- Discovered Vulnerabilities to MITRE (Common Vulnerability Database) and to third parties that provide products and services designed to detect vulnerabilities and malicious access attempts to assist third parties in developing more robust capabilities.

- Incidents related to a breach are reported to state and federal authorities as required.

- Threats and vulnerabilities that may potentially lead to exposure of critical infrastructure systems and infrastructure are reported to state and federal law enforcement authorities.

- The information reported can be detailed information regarding vulnerabilities, imminent or potential threats and successful intrusions or incidents, as required, and depending on the sensitivity of the information.

It should be noted that, as a state-regulated entity, we are required by law to provide information to the California Public Utilities Commission (CPUC) and its staff, upon request. Under law, any information provided to the CPUC must be open to inspection by the public, unless exempt from such inspection. Currently, there is no state law that specifically protects the confidentiality of critical energy infrastructure information or precludes its disclosure under the state's Public Records Act. While we request that the CPUC protect the confidentiality of critical energy infrastructure information at the time the information is provided, the CPUC is not required to inform us of subsequent requests under the Public Records Act for such information or provide notice of publication of the information. Thus, we can no longer control the disclosure of critical infrastructure information, once it has been provided to the CPUC. To ensure the protection of critical energy infrastructure information, any national or international standards would need to be applicable to state as well as federal agencies and authorities.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

National and international standards and organizations that develop standards can play an important role by helping to align the multitude of existing and developing cybersecurity standards and regulatory requirements. International Standards should play a major role in this process. Foreign and international laws should stipulate ownership and authority over enforcement actions, legal action, recourse, etc. Many of the attempted or successful breaches of Unites States based systems originate from foreign countries where no legal recourse exists, which leave organizations vulnerable to long term exposure. Additionally, those standards should establish appropriate requirements and standards for information sharing as well as incident handling. Local and federal government entities should be required to adopt the same handling requirements expected of corporate entities. The standards should be auditable by independent entities or accounting firms. Auditing should not be performed directly by international standards bodies or government agencies.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions. NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

1. What additional approaches already exist?

Risk Management approaches have been developed by many industry verticals but currently there is no cohesive approach that can be adopted uniformly and measured across the industry in general. Recently, a few organizations have developed a risk management approach for critical infrastructure but this approach provided little value in that it could not be leveraged holistically across an enterprise. Critical Infrastructure systems and infrastructure are part of system related to business process designed to provide products and services. Infrastructure components cannot be decoupled without consideration for the business process.

2. Which of these approaches apply across sectors?

Currently, there is no single approach other than cybersecurity frameworks and potential works by ISO and NIST related to risk management that could apply across sectors. The United States is one of a few countries that has not adopted a common approach to assessment, measurement and certification of a risk management. Cybersecurity is merely a risk discipline and should be handled in the context of an overall Risk Management program. British Standards (BS) and ISO standards are commonly adopted overseas.

3. Which organizations use these approaches?

We are not aware of specific organizations that use these approaches. None of the frameworks or approaches for Risk Management are mandated at a federal or state level.

4. What, if any, are the limitations of using such approaches?

There are several limitations of using existing approaches. First, many of these approaches focus on compliance objectives as opposed to risk outcomes. In addition, many have not been adopted successfully due to the lack of documentation on how to implement, use and or manage the approach. To seek expertise is typically very costly and not affordable for smaller companies, especially those developing point solutions. Additionally, because of the lack of guidance on how to properly implement a program, inconsistencies make it difficult to measure across the industry.

5. What, if any, modifications could make these approaches more useful?

In order to make these approaches more useful, consideration should be given to providing a means to lower the cost of implementation through tax incentives/rebates for adhering to better design principles. Additionally, stronger documentation and more flexibility for an organization to determine the most effective treatment of risk through a catalog of recommended controls. Corporations should be granted the flexibility to make the most prudent treatment decision based on a defined framework, but also incentivized by providing liability protection for corporations that operate at lower risk profiles than others in the industry.

6. How do these approaches take into account sector-specific needs?

An appropriate Risk Management framework considers that risk areas are multi-dimensional and provides an appropriate construct for organizations to make risk treatment decisions by applying the appropriate process and technology controls to minimize risk. Measurement is achieved by evaluating the residual or resulting risk after treatment or if untreated. This model provides the flexibility to be adaptable to any risk situation.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

A voluntary program for development, with incentives to participate, could ensure that all industry verticals are represented in the development of a holistic control framework as long as the incentives apply to all industry areas. Requirements can be generalized, but the standards should provide more than one choice to address the same situation, and the resulting outcome should also be flexible; i.e. the choice to manage to a low or medium risk for a particular situation. Additionally, more R&D funding and grants should be provided for academic and laboratory research to develop new and innovative approaches cybersecurity technologies that are more integrated with business process.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Sector-specific agencies and related coordinating councils can play an important role by participating in its use and administering training, education and awareness into the programs. There is also additional benefit they can add, by providing oversight to third party auditing firms to ensure fair and accurate reporting and certification administration of the program. Agencies and governance organizations should also exert influence on vendors to improve products where security is deficient, which is common in the industry

9. What other outreach efforts would be helpful?

Education, training and awareness would be helpful. Many organizations understand that frameworks exist, but not many really understand how to apply and use them. Additionally, local and federal government entities should put in place a consumer outreach program to educate consumers or cybersecurity best practices and risks.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

1. Are these practices widely used throughout critical infrastructure and industry?

The core practices identified by NIST are widely used throughout the industry, but they are not unique to critical infrastructure. Risk Management process includes the following process, at a minimum, that are common across all industry verticals: Strategic Planning, Capital Planning, Project Planning, Development, Integration, Monitoring and Incident Response. The same argument applies internally to organizations as well. IT/Cybersecurity Incident Response process is no different than the incident response process for dealing with outages.

Regarding privacy, the Generally Accepted Privacy Principles, and high level best practices like Privacy by Design, are used by government organizations as well as the private sector to effectively manage privacy concerns.

2. How do these practices relate to existing international standards and practices?

The core practices relate to existing international standards and practices in that they are applicable to any vertical industry.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

The practice that we see as the most critical for the secure operation of critical infrastructure is the Incident Management process, because technology solutions are at best capable of only chasing a problem. A good incident response program can account for many technology and process gaps to identify, contain and mitigate potential problems. An effective incident management process is the most important cybersecurity process.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

The practices are applicable for all sectors, with the exception of the security engineering process, which is not unique but rather a spinoff of standard industry audit and risk assessment processes. The value engineers provide is the ability to identify and correct potential weaknesses before introduction into a production environment. The process at its core is a combination of audit process and security design activity, the only potentially unique aspect is the controls.

5. Which of these practices pose the most significant implementation challenge?

Our organization believes that access control, in addition to internally controlling access, poses the most significant implementation challenge, because the industry lacks a common solution to be able to federate effectively across companies. Access control is also very difficult to implement given the nature of how data is used, stored and transported in today's technology era. Commonly used equipment in natural gas Industrial Control System environments often do not support centralized authentication and access controls that are consistent with current technology standards. Moreover, as noted above, as regulated entities, SDG&E and SoCalGas are required to provide state regulators and their staff access to our information.

Privacy also poses a challenge to implementation because privacy is poorly understood in many sectors and is often sacrificed in the name of security. Privacy by Design tells us that providing good privacy while implementing good security need not be a zero-sum game, that we can have both privacy and security if solutions are applied creatively and thoughtfully.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

We define requirements that map to standards (controls) that are specific to the organizational standard. The standards also define the appropriate implementation and testing procedures to ensure the control is operating effectively

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Our company has a methodology in place for the proper allocation of business resources to invest in, create and maintain IT standards. Throughout the industry, this is typically implemented through various assessment and compliance activities.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Our organization has a formal escalation process to address cybersecurity risks that suddenly increase in severity both through an incident management and handling process as well as through standard risk management process.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

To answer that question, we must first describe what privacy is. Privacy is the freedom to make personal decisions without unwanted influence. Privacy is peace of mind in knowing that personal information about us will not be used against us or those we care about. Privacy is sometimes simply about being left alone. The application of intrusive security practices—especially in the energy sector—can have strong negative and long-lasting impacts on an individual's energy privacy. In California, the use of smart meters by utilities to collect energy usage information from individuals is optional. Consumers may opt out of having a smart meter. If enough consumers decide to opt out, then all parties (customers, utilities, new third party markets, and the state) lose the benefits of this technology to meet the state's energy goals, provide new energy products and services, and reduce rate payer energy costs. It is essential for the energy industry to develop a culture of trust with energy consumers by advocating for and enabling consumer privacy in this space.

Privacy is concerned with offering individuals *transparency* in understanding how their personal information is being used and *choices* (i.e., control) about what and how information is being collected, how it's being used or whom it's being shared with. The act of implementing strong and reliable privacy measures helps to ensure that we maintain trust with individuals whose personal information and privacy is at stake. Without trust, Smart Grid will not meet its full potential and we will become less effective at securing critical infrastructure in a free society.

The Generally Accepted Privacy Principles and Privacy by Design address common privacy concerns, such as data minimization; management; notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security; data quality and monitoring and enforcement are important concepts to protect privacy. Each of these is required to adequately protect privacy and lack of attention to any of these represents a threat to individual privacy and should be addressed as part of a national standard. It is important to state that there's no need to re-invent the wheel here. There are plenty of good privacy principles and standards to choose from without having to invest a lot of energy in creating yet another set of standards for public and private organizations to follow.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

If the Framework is appropriately designed, we do not see any international implications on our global business or policy making. The European Union generally has more stringent controls on privacy that we would want to ensure at the least are not conflicting, and at best are well aligned with the framework we develop here.

11. How should any risks to privacy and civil liberties be managed?

Risks to privacy and civil liberties should be managed the way any other risk should be managed; by ensuring that appropriate controls are designed, implemented and monitored for effectiveness. Most importantly, those risks should be discussed openly and the concerns of interested stakeholders taken seriously when developing mechanisms to minimize those risks. Privacy has become too important to ignore.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

We believe that the answers provided to the RFI questions have allowed our company to adequately communicate the key points we believe should be taken into consideration for the development of this framework.

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, Information Security Manager, SKing@semprautilities.com, 858-613-5718.