Pacific Gas and
Electric Company

James W. Sample
Chief Information Security Officer
77 Beale Street, Mail Code B26S
San Francisco, CA 94105
J31K@pge.com

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The Pacific Gas and Electric Corporation (PG&E Corporation) is pleased respond with comments to the Request for Information issued by the U.S. Department of Commerce, National Institute of Standards and Technology, in the Federal Register on February 26, 2013, seeking input on “Developing a Framework To Improve Critical Infrastructure Cybersecurity”.

PG&E Corporation, incorporated in California in 1995, is a holding company that conducts its business through Pacific Gas and Electric Company ("Utility"), a public utility operating in northern and central California. The Utility generates revenues mainly through the sale and delivery of electricity and natural gas to customers. The Utility served approximately 5.2 million electricity distribution customers and approximately 4.3 million natural gas distribution customers as of December 31, 2011.

<u>Current Risk Management Practices</u>

NIST is soliciting information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and their management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/ or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST’s goal of developing a Framework that includes and identifies common practices across sectors.

1. Following are the greatest challenges PG&E sees in improving cybersecurity practices across critical infrastructure:

- Ability to receive and provide current, actionable threat, attack, intrusions, warnings and vulnerability information so mitigation measures can be implemented in a timely manner. An efficient means of information sharing is necessary between the private sector and government sources, as well as within the industry.

- The need for a single set of well maintained, sector agnostic security practices that third parties adhere to when providing products and services to critical infrastructure customers
    - Legacy utility assets lack current cybersecurity controls, and enhancements are costly.
- Improved commerce controls are needed in the supply chain when procuring goods and services from foreign countries
- Ability to use federal government capabilities for background investigations of employees operating in sensitive roles
- Identifying a risk management and compliance framework that focuses on risk based outcomes versus compliance mandates and objectives
- The need to develop of a comprehensive framework applicable across a diverse set of critical infrastructures and assets
- Education agendas, and a general culture shift, which ensure employees are trained and aware of the importance of their role in protecting critical infrastructure.
- Obtaining personnel with a skill set that includes both knowledge of utility operations and cybersecurity.
- Organizations overcoming a lack of commitment and priority to secure critical infrastructure

2. PG&E sees the following challenges in developing a cross-sector standards-based Framework for critical infrastructure:

- Ensuring that while appropriate security controls are identified, they aren’t so prescriptive as to negate the intent of securing critical infrastructure and information systems.
- In some cases a “one size fits all” framework may not achieve the intended results as it may be a “mile wide and an inch deep”. Due to the uniqueness of the various Critical Infrastructure sectors, security measures deemed essential to one may not be essential to others. A very fine balance must be identified.
- Integrating multiple requirements from legislation and regulatory requirements into a single body of standards applicable across sectors.
- Ensuring that appropriate safeguards and controls are implemented to enable information sharing across public and private sectors, while protecting confidential information from disclosure.
- Cyber threats evolve at a very rapid pace, making timely communications and incident response both within and across sectors critical
- Ensuring that overly prescriptive or duplicative requirements aren’t introduced and detract from the goal of securing critical infrastructure from a risk and cost based perspective.

3. PG&E corporate policies drive our risk governance model. Enterprise Technology Risk Management (ETRM) identifies security controls required for compliance with our policies and standards, and communicates them to the organization for implementation. Senior management is responsible for the implementation and support of these policies and standards. Procedures are then implemented that tie back to the required controls. Incident response plans are also a critical element associated with cybersecurity, and are incorporated into the organization's emergency response plans. It is also important to note that cybersecurity risk at PG&E is identified as an enterprise risk and is monitored by our Board.

4. At PG&E, ETRM is the organization responsible for overseeing the cybersecurity risk management program, and reports to the Senior Vice President for the Information Technology division.

5. PG&E evaluates risk based on loss and/or negative outcomes of financial and non-financial events. Risk is assessed based on measurement of the effectiveness of controls in place to manage that risk. ETRM has specific Risk Advisors assigned to each line of business, ensuring a solid understanding of risks and a direct line of communication.

6. At PG&E, cybersecurity risk is incorporated into organizations' overarching enterprise risk management, given that cybersecurity is regarded as one of the organization's greatest risks. Additionally, annual risk planning sessions occur involving all lines of business, ETRM, Enterprise Risk Management, and Executive Management, ensuring that adequate resource planning is performed based on the organizations risk portfolio.

7. PG&E has adopted best practices from numerous industry sources, via the Unified Control Framework (UCF), which include AGA, NERC, NIST, HIPAA, FAA, ISO and other national and international industry organizations, in order to understand, measure, and manage risk at the management, operational and technical levels.

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

- The electric sector must comply with NERC CIP and NRC requirements.
- Natural gas utilities do not currently have regulatory reporting requirements.

9. There are many organizational critical assets which are interdependent upon other critical physical and information infrastructures. Some examples include dependencies between natural gas and electric power generation, and all sectors generally rely on the

telecommunications sector for command and control of critical assets, as well as general operations.

10. Performance-based risk management goals are tied to reliability of service, safety, and cost to the end consumer, which ensures PG&E is able to provide essential services while managing cybersecurity risk. Organizational goals are tied to business strategy, which is informed by risk management, and propagated down through individually assigned goals. Those goals ensure risk and compliance activities are managed as expected.

11. Following are the regulatory bodies that PG&E reports to:

- NERC CIP: Annual self-certifications are submitted to WECC detailing how we meet requirements. Formal audits are conducted once every three years, and self-reports are required when controls are not being met. This process has been occurring since 2009 and is continually maturing.
- NRC: As an operator of a nuclear energy facility, PG&E is also subject to extensive regulation by the Nuclear Regulatory Commission (NRC) to ensure cyber protection.
- SOX: Quarterly control testing occurs, and the Finance VP submits related test result filings with the SEC. The SOX process has matured over the past eight years of operation.
- HIPAA: Control violations are reported if they occur.
- FAA/FCC: Control violations are addressed if they occur.
- Customer Privacy: Customers are notified of privacy violations in conjunction with PG&E policies and standards, as well as California state requirements. An anual report is sent to the CPUC.

12. National/International standards and organizations should provide the basis of critical infrastructure cybersecurity requirements, due to the breadth of experience and knowledge that can be provided by those organizations in establishing comprehensive security controls. They can play an important role in helping align the numerous existing and developing cybersecurity standards and regulatory requirements. Additionally, having a body that can guide improvements across sectors, and guide organizations to be successful with complying with the requirements would be beneficial. The standards that this body develops should establish appropriate requirements and procedures for information sharing as well as incident handling. Conformity assessments should be conducted by individuals with a strong understanding of the context and meaning of the security controls being tested. Additionally, continual improvements should be made to the requirements to both

avoid conflicts between “interpretations” and “letter of the law” issues, and determine where frequent interpretation issues are occurring based on assessment metrics.

Furthermore, foreign and international laws should stipulate ownership and authority over enforcement actions, legal action, recourse, etc. Many of the attempted or successful breaches on US based systems originate from foreign countries where no current legal recourse exists, leaving organizations vulnerable to long term exposure. Additionally, many sectors cross international boarders, such as Mexico and Canada, and should be considered when creating a framework.

Use of Frameworks, Standards, Guidelines, and Best Practices

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 is seeking 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.
NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

1. Approaches that already exist include:

- The Unified Control Framework (UCF), which PG&E leverages, provides a collection of controls across all industries and national/international standard groups. This framework allows a single, maintained view of mandatory and best practice controls to select from.
- A sector agnostic, successful control frameworks is ISO 27001. ICS-CERT alerts and best practices, and NIST standards provide a breadth of information as well.
- AGA members are encouraged to utilize the TSA Pipeline Security Guidelines and most of its members currently use these guidelines or are evaluating them for use.

2. The first two approaches above apply across sectors.

3. PG&E leverages the above approaches, as do many organizations. All critical business functions leverage these practices at PG&E.

4. One limitation of using such an approach is that additional analysis must be performed to determine which controls are applicable to an organization: all may not

apply. Based on the applicable subset, maintenance activities must be performed to ensure controls remain current. Additional limitations include the focus on compliance objectives opposed to risk outcomes, and not all approaches are cost effective to all sectors.

5. One modification that would make these approaches more useful would be clearer documentation, as well as adding more flexibility for an organization to determine the most effective risk mitigation through a variety of possible compensating controls based on a high-level framework.

6. In order to take into account sector specific needs, the Risk Management framework should consider that risk areas are multi-dimensional and provide capabilities for organizations to make risk based decisions by applying process and technology controls to minimize risk. This provides a scalable, flexible approach that can be applied to any risk situation. Using international and national standards, such as ISO 27001 and NIST standards, each sector must determine how to integrate controls to best reduce risk in their environment.

7. Standards development for use of existing frameworks should take into account sector specific issues and remain voluntary to ensure asset owners are able to provide reliable, safe and cost effective services. Feedback through voluntary programs allows the further refinement of standards development.

8. The sector-specific agencies and related sector coordinating councils encourage companies to implement these approaches and best practices by fostering an information exchange and sharing environment.

9. Other outreach efforts would be helpful include:

- Public-Private coordination to ensure a successful implementation of the framework and information sharing.
- Requirements should be closely aligned with other mandatory requirements and industry guidance provided by regulatory bodies and sector specific agencies.
- Education, training and awareness in the form of workshops, webinars and tutorials are outreach efforts that would be helpful.

Additionally, following are a list of incentives that would assist in making outreach efforts more attractive to organizations:

1. Expedited Security Clearance Process
2. Grants

3. Include Cybersecurity in Rate Base
4. Information Sharing
5. Insurance
6. Liability Considerations
7. New Regulation/Legislation (e.g. Cyber SAFETY Act)
8. Prioritized Technical Assistance
9. Procurement Considerations
10. Public Recognition
11. Security Disclosure
12. Streamline Information Security Regulations
13. Subsidies
14. Tax Incentives

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. Standard practices have been established in the electric sector based on NERC requirements to protect critical infrastructure, as well as general best practices established using NIST standards. These core practices identified by NIST and NERC are not unique to critical infrastructure.

These practices are also mature and incorporated in documents such as TSA’s Pipeline Security Standards and INGAA Cybersecurity guidelines which are used by AGA members.

2. The basis of NERC requirements were established by industry experts and their knowledge associated with international standards and practices. These standards and practices are not applicable to only the electric sector.

3. Collectively, the practices comprise a complete program for managing enterprise risk within critical infrastructure, in any sector, and should be applied using a risk based approach. The following practices are seen as being the most critical for the secure operation of critical infrastructure from PG&E's perspective:

- Incident handling policies and procedures,
- Asset identification and management,
- Incident handling policies and procedures, and
- Identification and authorization of users accessing systems

4. At a high-level, the guidance and practices may be applied across all sectors. All organizations should evaluate these practices using a risk-based approach to determine if the practice is applicable or not. Applicability of these practices may vary across organizations in a specific sector based on risk factors.

5. One significant implementation challenge specific to utilities includes the fact that industry equipment used in control system environments often does not support current technology standard security controls, including centralized authentication and access models.

6. International standards such as NIST and ISO 27001 provide a well-developed and maintained set of best practices that organizations can apply when meeting regulatory requirements as well as during the development of internal policies and standards.

7. Many utilities are staffed for the creation and maintenance of IT standards. Regular maintenance of these standards has been challenging for many organizations, and smaller organizations may be challenged to provide resources to support this function.

8. PG&E has a formal escalation process to address cybersecurity risks that suddenly increase in severity through established incident response processes incorporated in emergency response plans. Both internal monitoring and external alerts feed into these processes.

9. Organizations must classify and protect confidential and restricted data as per national and state law, and the utility industry has a commitment to protect customer privacy. While access controls are included in most frameworks, not many of the current

industry requirements speak to privacy concerns. States already have existing privacy and breach laws that provide coverage for personally identifiable information. Further, the DOE and NIST consultative processes should be encouraged to continue.

10. Given that gas and electric infrastructure extends into Canada and Mexico, international implications of this Framework should be considered in policymaking.

11. 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.

12. In addition to the practices noted above, considerations to include education and tabletop exercises should be made.

Thank you for providing PG&E the opportunity to provide comments, and we look forward to further developments in this important area.

Regards,

James W. Sample
Chief Information Security Officer