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

Dear Ms. Honeycutt,

Thank you for the opportunity to provide information regarding the cyber-security standards and practices of CenterPoint Energy, Inc. ("CenterPoint Energy").

CenterPoint Energy, headquartered in Houston, Texas, is a domestic energy delivery company that includes electric transmission & distribution, natural gas gathering, processing and distribution, interstate pipelines and competitive natural gas sales and services and has assets totaling more than $21 billion. Our company has 8,800 employees and serves more than 5 million metered customers primarily in Arkansas, Louisiana, Minnesota, Mississippi, Oklahoma and Texas.

We take seriously the responsibility of protecting our customers, employees, assets and the communities in which we operate and thus cyber-security is a top priority for CenterPoint Energy. Not only is it a matter of focus for our senior management, we periodically brief our Board of Directors regarding our cyber-security activities.

CenterPoint Energy has established a cyber-security policy and set of practices and continuously works to improve our cyber-security practices and protocols. As threats have evolved, we have increased the resources in our company with designated responsibilities for varying aspects of cyber-security. We understand that the accelerating pace of change in the cyber-security space requires orchestrated collaboration both internally and externally. The development of our practices has involved active participation across our business units, industry, standards and regulatory groups, as well as extensive collaboration with our suppliers, regulators and various branches of the federal government.

As a company that comprises several business units that own and operate critical infrastructure, we understand the importance of vigilance in the face of varied and evolving cyber threats. Accordingly, we have collaborated with (and continue to work with) the federal government, state regulators, various outside companies, and industry associations to develop and maintain our cyber-security practices. Among them are the American Gas Association ("AGA"), the Interstate Natural Gas Association of America ("INGAA"), the Electric Power Research Institute ("EPRI"), the Edison Electric Institute ("EEI"), the National Institute of Standards and Technology ("NIST"), the North American Electric Reliability Corporation Critical Infrastructure Protection Committee ("NERC CIPC), the Department of Energy ("DOE"), the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security ("DHS"), the Transportation Security Administration ("TSA"), the National Electric Sector Cyber-Security Organization Resource ("NESCOR"), Idaho National Laboratory ("INL"), Pacific Northwest National Laboratory ("PNNL"), and numerous city and county governments across our footprint. We are regulated by federal and state agencies that have a keen interest in operational safety and cyber-security including, for example, the Federal Energy Regulatory Commission ("FERC") and Public Utility Commission of Texas ("PUCT"). And, as required by CenterPoint's SmartGrid grant, the Department of Energy reviews our cyber-security practices and plan annually.

Current Risk Management Practices

What do organizations see as the greatest challenges in improving cyber-security practices across critical infrastructure?

- Establishing a comprehensive frame work across a diverse set of assets.
- The cost of improvements to legacy assets.
- Continuing need to ensure cyber-security technology for proprietary assets is available and up to date.
- Challenges associated with ensuring work force possess skill sets critical to utility operations and cyber-security. Ongoing workforce development is critical.
- Need for timely threat information specific to industry.
- A risk management and compliance framework that assesses risk based on outcomes versus compliance mandates and objectives.

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

- Developing a frame work that will be applicable to a diverse set of assets.
- Coordinating cross sector collaboration.

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

- CenterPoint Energy has an enterprise risk management organization that utilizes the Committee of Sponsoring Organizations COSO risk management framework.
- Cyber-security has been identified by the ERM as an independent risk, which is rated among the highest of identified risks to the organization.
- The ERM process establishes communication across the enterprise and ultimately reports to the highest levels of senior management and the Board of Directors.

Where do organizations locate their cyber-security risk management program/office?

- The cyber-security risk management program is located in the ERM Office and has senior level participants from across the organization.

How do organizations define and assess risk generally and cyber-security risk specifically?

- Risks are defined using the COSO framework and the ERM process.

To what extent is cyber-security risk incorporated into organizations' overarching enterprise risk management?

- Cyber-security is fully incorporated into the ERM program and has been identified as one of the highest independent risk to the organization. Cyber-security has also been identified by the ERM as a risk to most of the large projects and programs that contain cyber assets.

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

- CenterPoint Energy has a comprehensive ERM program utilizing the COSO framework.
- CenterPoint Energy is an integrated energy utility with a diverse set of assets. All applicable standards, best practices, and tools are evaluated to determine applicability for managing cyber-security risks.
- Standards and best practices that are currently utilized by CenterPoint Energy include but are not limited to NIST, Institute of Electrical and Electronics Engineers ("IEEE"), Control Objectives for Information and Related Technology ("CobIT"), NERC CIP, and Information Technology Infrastructure Library ("ITIL").

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

- NERC CIP, Sarbanes-Oxley Act ("SOX"), Health Insurance Portability and Accountability Act ("HIPPA"), PCI, DOE for grant recipients, FERC, Transportation Security Administration ("TSA"), Public Utility Commissions, and City and County governing bodies.

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

- Most critical assets in the utility industry are interdependent upon all of the other critical physical and information infrastructures including telecommunication, water, other energy organizations and transportation.

What performance goals do organizations adopt to ensure their ability to provide essential services while managing cyber-security risk?

- In the natural gas and electric utility industries all performance base risk management goals are related to reliability of service, safety, and cost to the end consumer.

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?

- CenterPoint Energy reports to many different local, state and federal governing bodies.
- Reporting mechanisms are usually dictated by the regulatory body and have different requirements.
- Where possible, CenterPoint Energy tries to have a uniform report for cyber-security reporting.

What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cyber-security conformity assessment?

- National/international standards committees should strive to develop cross sector standards that will be effective, efficient, and consistent for asset owners to implement and report on.
- National/international standards committees should fill the role of facilitators for cross sector collaboration in order to ensure the cyber-security framework meets the needs of each sector.

Use of Frameworks, Standards, Guidelines, and Best Practices

What additional approaches already exist?

- Comprehensive frameworks, standards, guidelines, and best practices already exist but need to be shared and consistently applied.

Which of these approaches apply across sectors?

- The more established approaches apply across industry sectors.
- If a risk-based model is used, most of the existing approaches can be applied across sectors.

Which organizations use these approaches?

- Natural gas and electric utility organizations

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

- Not all approaches will be cost effective for all sectors.

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

- Existing approaches to cyber-security can meet sector-specific needs if they are applied using a risk-based approach that is scalable and flexible.

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

- Standards development for use of existing frame works should take into account sector-specific issues and remain voluntary except where mandatory regulations already exist to ensure asset owners are able to provide reliable, safe and cost effective services.

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

- An important role of sector-specific agencies and sector coordination councils is to facilitate participation and adoption of standards and frameworks by sector organizations.

What other outreach efforts would be helpful?

- NIST should conduct cross sector workshops in the near future in order to gain timely input towards the framework by sector organizations.

Specific Industry Practices

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.

Are these practices widely used throughout critical infrastructure and industry?

- Yes, these practices are at a mature state throughout the natural gas and electric utility industries.
- These practices are used throughout our operational as well as business systems and are required by regulation in many areas of our industry.

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

- These practices are common throughout the industry.
- These practices are referenced in most standards and frameworks.

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

- These practices make up end-to-end programs for managing risk within critical infrastructure.
- All of these practices should be applied using a risk-based approach.

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

- Organizations that operate critical assets should evaluate all of the practices using a risk-based approach to determine if the practice is applicable or not.
- Applicability of these practices may vary across the organization in a specific sector based on risk factors.

Which of these practices pose the most significant implementation challenge?

- The challenges to implement these practices will vary across the organization in a given sector based on the current technology deployed, the rate base in a geographic region, and the regulatory requirements of a given organization.

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

- Standards and guidelines are used to define how a given practice is applied to varying technology throughout an organization.
- Guidelines are used as a reference for best practices and provide a method to measure implementations.

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

- In the natural gas and electric utility sector large organizations do have resources currently assigned to create and maintain IT standards. These standards and associated utilized processes are regularly audited for compliance in most large utility organizations.
- Smaller municipal or cooperative organizations may have challenges allocating resources to development and maintenance of IT standards.

Do organizations have a formal escalation process to address cyber-security risks that suddenly increase in severity?

- CenterPoint Energy has a formal escalation process to address cyber-security risks. This process is part of the CenterPoint Energy Cyber-Security Incident Response Plan, which is a component of the Business Continuity Plan.

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

- If applied correctly, these practices should not impose any risk to privacy or civil liberties.

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

- CenterPoint Energy is a domestic energy delivery company that only operates assets within the United States.

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

- Risks to privacy and civil liberties should be handled within the regulation and standards that apply.

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

- Cyber-security awareness should be made a part of ongoing workforce training and development for all critical infrastructure sectors, if it is not already incorporated into cyber threat management programs.

In conclusion, I want to stress that CenterPoint Energy appreciates the very real nature of these threats and stands ready to work with you to address cyber vulnerabilities. We welcome additional opportunities to discuss these matters with you and your staff. Should you have any questions, please do not hesitate to contact me.

Sincerely,

Mike Phillips
Corporate Information Security Director
CenterPoint Energy
713 207-7054
Michael.phillips@centerpointenergy.com