Gary W. Hayes

Division Vice President & Chief Information Officer

CenterPoint Energy, Inc.

****

Testimony before the House Committee on Homeland Security

****

"DHS Cyber Security: Roles and Responsibilities to

Protect the Nation's Critical Infrastructure"

March 6, 2013

Overview

Chairman McCaul, Ranking Member Thompson, and Members of the Committee, my name is Gary Hayes and I am the Chief Information Officer for CenterPoint Energy. Thank you for inviting me to testify on my experiences and perspectives on protecting critical infrastructure from cyber attacks.

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

As the CIO of CenterPoint Energy I am accountable for our cyber security programs and have direct responsibility for our corporate business systems' cyber security. Because of the diverse segments of the energy infrastructure in which CenterPoint Energy's companies participate, I coordinate, collaborate, and communicate with our operational technology functions to define policies, procedures, practices and programs in our efforts to provide cyber security. I have a highly dedicated, educated and capable team executing responsibilities in this effort.

I also have the responsibility to represent and coordinate representation of our company in industry and government efforts focused on cyber security.

We focus heavily on participation in relevant industry groups. I participate on the American Gas Association ("AGA") and Edison Electric Institute ("EEI") Cyber Task Groups and I coordinate with David Jewell, Senior Vice President, Commercial Operations, Optimization and Gas System, who represents CenterPoint Energy on the Cyber Task Group for the Interstate Natural Gas Association of America ("INGAA"). We also participate in numerous governmental, private and industry-related efforts focused on cyber security.

Our cyber security technologies operate across three areas: interstate pipelines, local gas distribution utilities and an electric utility. For cyber security purposes, our interstate natural gas transmission pipelines are under the jurisdiction of the Transportation Security Administration ("TSA"). Our local gas distribution companies operate under the same jurisdiction but, for cyber security purposes, have no single regulator because some of the Federal authority has been delegated to the states. And, finally, CenterPoint Energy's electric utility in the Houston, operates under the jurisdiction of the Federal Energy Regulatory Commission ("FERC") for compliance with North American Electric Corporation reliability standards. We also work voluntarily with a multitude of other groups including the Federal Bureau of Investigation, Industrial Controls Systems Cyber Emergency Response Team (ICS-CERT) and the Department of Energy (DOE) and, of course, Department of Homeland Security (DHS).

My goal today is to share CenterPoint Energy's perspective with regards to cyber security challenges, activities and opportunities. That perspective is this: cyber threats are evolving and require collaboration, information sharing with the government and continued collaboration with the industry to effectively protect the nation's critical infrastructure. Our goal is to focus our resources on facing the cyber threat.

This perspective is shaped by our experiences and participation in industry groups as well as our collaboration with several governmental agencies including the DOE, DHS and the TSA. Furthermore, our relationship with members of our supply chain, our suppliers and vendors, is critical. From these experiences, we have determined that we need the ability to respond in a quick and agile manner, as well as continuously improve our capabilities to respond. Collaboration is the key.

As a critical energy transporter and distributor to the nation, we know that we have responsibilities to the public, our customers and our shareholders. We have prioritized our cyber security efforts in parallel with our corporate philosophy.

1. Public Safety

2. Energy Delivery

3. Customer Service

I hope this document provides a helpful "participant's view and perspective" as we work together to protect our Company and our nation's critical infrastructure.

Cyber Security Efforts and Collaboration

CenterPoint Energy has a long history of safe and reliable energy delivery to our customers. Our team members take pride in getting up every morning with this mission top of mind. To this point, we take protection of the public, our control systems, customer and employee information, critical infrastructure information, and intellectual property very seriously. Cyber security has been incorporated into our processes, procedures, and operations through various mechanisms over time. But, we do recognize that the current cyber environment has escalated beyond historical expectations and our efforts must and will continue to evolve in order to meet these dynamic and ever-evolving threats.

We have evolved from a strategy of "perimeter defense" (e.g., keep the bad actors out) to a strategy of "depth-in-defense" (recognition that technology system perimeters were susceptible to compromise, depth-in-defense provides increased reliance on detection and response mechanisms to address threats within the protection perimeter). We have established objectives, techniques, talent and tools to assist us in our current efforts. We have also focused on educating our workforce, as they represent the first line of defense. However, we recognize our cyber security capabilities must continue to evolve. This recognition comes from education and collaboration with industry and government. Our objectives are to mature and enhance our strategy and move to an "agile defense".[1] In particular, we will enhance our focus on the people, processes and technologies that can be managed, monitored, tested, measured and continuously improved.

As an important part of the energy delivery value chain, we are also enhancing resiliency, which is our ability to respond quickly to attacks and to maintain critical services. As we have learned through our participation in many of the cyber discussions, "bad actors will get in". It is not a matter of "if" but a matter of "when." Therefore, we continue to evolve our capability to respond and operate in a compromised state.

Identifying and coordinating with the right stakeholders is vital to that evolution.

[1] An enhanced comprehensive security strategy referred to by NIST as "agile defense". Agile defense combines traditional perimeter, depth-in-defense and depth-in-breadth, which is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the life cycle. Life cycle is the network that includes product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement.

First, we believe that participation with industry coalitions is critical. Our collaboration with fellow energy sector members allows us to continually learn and incorporate leading practices, provide mutual assistance and educate stakeholders and policy makers of real risks and possible solutions. We encourage and assist in collaboration between AGA, EEI, INGAA and key policymakers.

Second, collaboration between the public and private sector is a vital part of cyber protection. Deployment of the SmartGrid in Houston presented us with the opportunity to work with DOE, DHS and other federal agencies in order to successfully deliver advanced metering capabilities. Throughout the process, we collaborated with government stakeholders to incorporate customer protection and cyber security into our design and operations. This could not have been achieved without information sharing, a focus on quality and integrity, strong risk management, and joint objectives - all of these achieved through collaboration.

Those partnerships are also critical for our intelligent grid project and we look forward to continuing those relationships.

Other examples illustrating the success of public-private partnerships are the joint industry and governmental initiatives that developed the electric sector cyber security Capability Maturity Model, guidelines for the natural gas pipeline sectors' Pipeline Security Guidelines and many more activities that have benefited CenterPoint Energy and our industry. These collaborative efforts focused on targeted objectives and provided tangible programs, information, tools, techniques, and knowledge to help us enhance our efforts in this war against cyber threats. We encourage Congress to promote continued focus on private and public partnerships for the protection of our national security.

And, finally, cyber security collaboration must take into account the entire life cycle and supply chain. Therefore, we must recognize the essential participation of our vendors and suppliers in this effort. They have worked with us to provide products and solutions to meet the demands of this challenge. Our joint goals and efforts focus on design, testing, and improvement of products to understand quality, integrity, risks, threats, mitigations and management of these solutions in our operating environment.

Cyber Security Participant Observations

There is a set of common themes that we see emerging from our cyber security efforts and dialogues:

Shared Goals: Identifying and merging the focus and priorities of the stakeholders is a key to success.

Risk Based Approach: A risk based approach is fundamental to our efforts. Goals should be prioritized and articulated clearly. Solutions should be focused and yet flexible. A "one size fits all" approach won't work for unique problems. There are utility service providers serving hundreds of customers and others serving millions of customers; therefore, the risk profile will influence the objectives, techniques and tools to effectively manage cyber security.

Information Sharing and Situational Awareness: We desire a defined collaborative process to share information in a quick, secure and non-prejudicial fashion. That process should educate us in ways that we can be proactive and not reactive. Throughout many conferences, meetings, calls and other interactions, we continue to hear that the ICS-CERT serves as a strong template for developing a working model of collaboration. "Boots on the ground" security team members find this of great value in their efforts in the cyber war. We believe this is an example of information sharing that provides actionable information, support to our industry, and brings value to public-private partnership.

Leveraging Tools and Techniques: Although we, and many others, employ market-leading technologies and information solutions, we believe our effort would be greatly enhanced by leveraging cyber technologies and solutions utilized by governmental organizations and fellow industry members. We recognize there are many obstacles, but today's cyber security challenges require us to remove these obstacles and provide a repeatable and supportable path to facilitate results. Each day of delay is another day of opportunity for advanced persistent threat actors.

Security Clearance: Expanded security and expedited clearance for appropriate personnel within the private sector and expedited communication of critical information is critical to the ability of owners and operators to be proactive and responsive to emerging threats. We were pleased to see such a provision in the President's Executive Order on cyber security.

Cyber Security Regime: A cyber security framework must prioritize the principle that agility is the key to responding to cyber threats. An overly burdensome and prescriptive regulatory regime will be increasingly challenged to keep pace with evolving cyber threats. A beneficial framework not only defines capabilities, but provides learning, methodologies, objectives and techniques (tools and measures) to achieve the required results. In conjunction with risk-based analysis, that type of framework can be leveraged by all participants to mitigate threats.

Incident Management: The reality is advanced persistent threat actors are not going away and the risk of a cyber incident will remain top of mind for the foreseeable future. Increased situational awareness coupled with response and recovery plans will be incorporated into existing emergency operating procedures.

A leading effort on incident management comes under the auspices of the National Infrastructure Advisory Council (NIAC) report, several electric utility CEOs are engaged in an ongoing partnership with the White House National Security Staff and senior officials throughout the government, including Department of Energy Deputy Secretary Daniel Poneman and Department of Homeland Security Deputy Secretary Jane Holl Lute. This collaboration has resulted in several government-industry initiatives, one of which is to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

Collaboration: All of these themes require partnerships with industry and government. Collaboration is essential to our combined mission of protecting the public, customers, employees, critical infrastructure, intellectual property and national security. Notable examples demonstrating the strength of collaboration between public and private sectors include the Industrial Control Systems Joint Work Group (ICS-JWG) and the TSA-sponsored public-private partnership which supports the National Infrastructure Protection Plan (NIPP).

To illustrate further, I offer the case of our interstate gas transmission pipelines where the cyber collaboration with the federal government began through our work with INGAA and AGA. After the September 11 attacks, and before the TSA or the DHS were created, we voluntarily collaborated through INGAA and AGA with the then Research and Special Programs Administration within the Department of Transportation (DOT) to develop the initial Pipeline Security Information Circular. This collaborative approach to developing and implementing security measures continues to this day in our collaboration with the TSA. Since that time, gas pipeline owners and operators have worked with TSA to safeguard and protect our infrastructure's security – both from physical and cyber attacks. As a result of years of work and collaboration between owners and operators and the TSA we have a strong, trust-based collaboration – a public-private partnership. This approach, and the relationship it fostered, produced robust, thorough cyber guideline development for natural gas transmission pipelines even before the "911 Act" became law.[2]

TSA is using a voluntary partnership approach because it works. TSA and the private sector partner in order to leverage the collective expertise and experience of the government and private industry in finding practical solutions to cyber security. This approach and the relationship it has fostered have produced robust cyber security guidelines and best practices for natural gas transmission pipelines.

The TSA approach builds on what has been proven through experience: public-private partnerships for cyber security generate solutions. A Congressional Research Service August 2012 report, "Pipeline Cyber Security: Federal Policy," stated that "TSA officials assert that

[2] Implementing Recommendations of the 9/11 Commission Act.

security regulations could be counter-productive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments." Moreover, the report notes that "[b]ecause TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well."

We believe that the key to effective cyber security is the trust developed in partnerships like the one with TSA. The dynamic solutions that are born of the public and private sector coming together are not possible when the government is only acting as a regulator and enforcer. The cyber security world moves too quickly for such traditional regulatory models to be beneficial or productive.

Conclusion

We take seriously the responsibility of protecting our customers, employees, assets, and communities in which we operate, and thus cyber security is a top priority for CenterPoint Energy. We also recognize the importance of critical infrastructure to our national security. Because cyber threats are constantly changing and evolving, we support voluntary programs that encourage partnership, collaboration, sharing of information and technology, and the preparedness necessary to mitigate and respond to the ever changing nature of cyber attacks. We will not succeed in this effort alone. The strengthening and expansion of industry and government partnerships provides our best front in this cyber war.

Chairman McCaul, Ranking Member Thompson, and Members of the Committee, we appreciate the opportunity to share our perspectives and stand ready to assist you in your efforts to protect our critical infrastructure.