CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC'S COMMENTS ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INTERAGENCY REPORT 7628 (DRAFT): SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS

November 24, 2009

Overview of the Texas Electric Market

CenterPoint Energy Houston Electric, LLC ("CEHE" or "Company") is a fully regulated Transmission and Distribution Electric Utility ("TDU") whose rates, operations, and services are subject to the jurisdiction of the Public Utility Commission of Texas ("PUCT"). The structure of the Texas retail electric market is unique. Since 2002, electric utilities have been functionally unbundled, with utility functions separated into the following three components: generation, transmission, and retail sales. Of these functions, only the transmission and distribution functions remain subject to utility regulation; the power generation, wholesale sale of electricity, and the retail electric sales functions now operate in a competitive marketplace.

As a result of this restructuring, a competitive market for retail electric services now exists in the Electric Reliability Council of Texas ("ERCOT"), where retail consumers purchase electricity from among a large number of Retail Electric Providers ("REPs") that offer electricity at competitive prices with various service plans. In this environment, REPs purchase and schedule electricity from power generators based on their customers' expected usage, and TDUs like CEHE deliver electricity from electric generating facilities to retail consumers for REPs in their respective service areas. The Company, for example, provides TDU delivery services for approximately 30 REPs that actively market electricity to residential consumers on the PUCT's "The Power to Choose" website. REPs served by CEHE currently serve over two million retail customers across a 5,000-square-mile area along the Texas Gulf Coast, including the Houston metropolitan area, the Nation's fourth largest city.

CEHE's Comments on NIST 7628

IN GENERAL

The Company appreciates NIST's efforts in establishing the Smart Grid Cyber Security Strategy and Requirements, and we appreciate the opportunity to comment on NISTIR 7628 ("Draft Report"). The Company remains a leader in the electric industry in providing security for its operations and was encouraged by the guiding wisdom offered in Appendix A of this Draft Report: "Balance is needed between security measures and power system operational requirements. Absolute security may be achievable, but is undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. . . . Balance is also needed between the risk and the cost of implementing the security measures." The Company believes that balance is a crucial ingredient in ensuring any effective, successful security program, including a program related to cyber security for an electric distribution system.

-1-
The U.S. Department of Homeland Security (DHS) similarly emphasizes the need for balance in its control systems security recommendations,¹ which NIST referenced in creating its Draft Report. As part of its recommendations, DHS states that "[t]he goal of a control systems security program is to balance security while operating within resource limits. . . . Security is not to impede operation. . . . The most successful security program is one that integrates seamlessly and becomes a common aspect of daily operation."² As written, and at least in isolation, the Draft Report does not allow for much balance. That is, there is no rule of reasonableness to be applied by the utility, nor are alternative security measures contemplated that would provide adequate protection. To the contrary, it appears as if the requirements (and the supplemental guidance and enhanced requirements as well) outlined in the Draft Report are to be followed regardless of cost or other contravening measures.

Utilize Risk-Based Performance Standards.

In order to strike the right balance, it is imperative that any cyber security program be governed by risk-based performance standards, not by security-specific requirements. The Company cannot overstate the need for flexibility in reaching the desired security ends. The DHS recommendations, again, are instructive: "Decisions regarding when, where, and how these standards should be used are best determined by specific industry sectors. This document provides those decision-makers with a common catalogue (framework) from which to select security controls for control systems."³ Importantly, not just specific industry sectors but the companies themselves should play a significant role in deciding when, where, and how standards should be used. Give industry a desired end, and let it determine how best to get there.

The diversity of solutions offered by risk-based performance standards benefits the goal of increased security for other reasons. For instance, hackers may prove more effective homing in on prescriptive, detailed solutions published in the Draft Report, where they know exactly what they are confronting when attempting to disrupt a utility's Smart Grid.

Responsibility for Enforcement Authority Should Be Announced.

Although CEHE understands NIST's role in creating standards (or requirements), the Company is less clear which agency or agencies, and at which level (State or Federal), will have ultimate enforcement authority in this area. Without a named responsible agency, for instance, there can be no assurance that FERC/NERC will be the enforcement authority. Even assuming FERC will have enforcement authority, it is unclear whether another Federal agency, such as DHS, will have a coordinating role in crafting policy and regulations. The Company understands that there are several efforts ongoing at the Federal level to legislate cyber security. In the meantime, however, without knowing the amount of institutional knowledge the eventual enforcement authority will have, CEHE is without sufficient knowledge to best tailor its comments. Consequently, CEHE asks that it and others be given an additional opportunity to comment on

² Id. at 2 (underline added).
³ Id. at 1.
any standards, requirements, or regulations after jurisdictional issues at the Federal level related to cyber security are resolved.

Further, it appears as if there may be at least two sets of requirements emerging at the Federal level relating to cyber security—i.e., these NIST requirements and NERC-CIP requirements—as well as security requirements that exist at the State level. It is important that utilities such as CEHE be bound by only standards and requirements that are complementary. At the Federal level, the NERC-CIP standards already cover bulk electric transmission, so new requirements related to the Smart Grid should not be inconsistent or redundant.

Federal regulations in this area also raise concerns at the State level. For instance, the Draft Report and its use cases apply to a more traditional vertically integrated utility and make no allowances for the deregulated model in Texas. The language relating to Home Area Network ("HAN") devices which would place all security responsibility on the TDU is completely inconsistent with the existing Texas market, where many if not most of the IAN devices will neither be owned nor controlled by the TDU.

Employing a regulatory construct governed by risk-based performance standards provides a practical way to overcome these issues. Moreover, although CEHE has no objection to the Federal government having ultimate regulatory authority over cyber security of the Smart Grid—particularly with FERC/NERC as the Federal point of contact—the Company believes that State authorities should have the enforcement authority over the regulations.

*Audit Provisions Should Be Clarified.*

The Company believes that a few areas concerning audits in the Draft Report need revision and/or clarification. Throughout Section DHS – 2.16, for instance, the term “audit” is used to describe both management monitoring responsibility and independent audit activity. A more detailed definition of “audit” and “independent audit” is required. The same section mentions that audits “can be either in the form of internal self-assessment or independent, third-party audits.” Does this mean companies can choose which audit is performed? Similarly, regarding the language “selection of auditors”: Does this imply that companies will have the ability to select who will audit them? Finally, there is an apparent inconsistency arising from DHS – 2.16.14.1. This requirement seems to state that internal audits can perform reviews. This seems to conflict with DHS-2.16.11.2, which states independent reviews are required for audits beyond documentation reviews.

As to Section ASAP-2.16.13.2, which describes the measures that need to be taken to safeguard audit tools, is the Draft Report referring to audit tools used in monitoring activities (e.g., logs, reports, etc.) or tools used to conduct an audit (e.g., ACL, TeamMate, etc.)? Some of the tools that may be used to conduct an audit are available freely on the Internet (e.g., NMAP, Snort, etc.). How are companies supposed to “protect” these Advanced Meter Infrastructure (“AMI”) system audit tools from misuse or compromise?

*Certain Language in the Appendices Should Be Refined and Redefined.*

Appendix A states, in relevant part: “Power system operations must be able to continue during any security attack or compromise (as much as possible).” CEHE concurs with this statement.
The Company would emphasize, however, that it is unreasonable to think that all power system operations must continue during any security attack. This statement should be refined to demonstrate that some portion of a power system can cease operations without an objectionable impact on the overall power system.

Moreover, there are many locations in Appendix A where the term “critical to distribution operations” is used. This can be a misleading use of the term “critical” and confused with the use of the term “critical” in the NERC-CIP standards. For instance, “critical to the distribution system” is not necessarily “critical” to the Bulk Power System. CEHE therefore advocates the use of a different term.

Finally, on page D-15 of Appendix D, the last comment states: “There is probably a need for intersection of security at various layers.” The Company believes there is not only a need for security at various layers, but also within networks and—for example, in Texas where the data of different TDUs will be stored in the Smart Meter Texas Common Repository.

**CHAPTER ONE: CYBER SECURITY RISK MANAGEMENT FRAMEWORK AND STRATEGY**

Sec 1.3. The second bullet item on page 3 provides a definition of Cyber Security, and indicates that the definition is for this document. The Company believes that this definition is different than the NERC-CIP definition of Cyber Security, and that the definitions should be the same.

Sec 1.4. The Company proposes the following changes to this Section, which states, in relevant part: “The risk assessment process for the Smart Grid will be completed when the security requirements are specified. These requirements will be selected on the basis of a risk assessment and will apply to the Smart Grid as a whole. The requirements will not be allocated to specific systems, components, or functions of the Smart Grid. In specifying the security requirements, to the extent practical gaps will be identified. The implementation, assessment and monitoring of security controls are applicable when a system is implemented in an operational environment. The output from the Smart Grid risk management process should be used in these steps. In addition, if feasible, the full risk management process should be applied to legacy systems and when Smart Grid owners and operators implement new systems or augment/modify existing systems.”

The Company is not sure what is meant by “requirements... will apply to the Smart Grid as a whole” and seeks clarification. It is unclear whether this language implies that each utility segment, including individual meters, should be met with the same amount of security. Such an interpretation would be inconsistent with the Federal government’s security approach—and, indeed, this Draft Report—which is predicated on risk. Various segments of the Smart Grid clearly have different risk profiles. The most obvious example is the individual meter, which poses much less risk to the Smart Grid than, for instance, a unit in the transmission system. Therefore, each segment within the Smart Grid should be secured based on the amount of risk it poses to the Smart Grid.

Moreover, Section 1.4 of the Draft Report implies that all standards are specified by a risk analysis, which is not necessarily correct. The language does not allow utilities to perform their own risk analysis, yet seems to indicate that this NIST document can prescribe all of the
necessary cyber security requirements. It appears as if, by stating that NIST will identify all standards and gaps, there is no need for utilities to complete their own analysis and simply accept the one-size-fits-all approach. CEHE strongly recommends that NIST acknowledge the inherent cyber security value of allowing multiple approaches to meet common performance goals over a one-size fits all approach, and the role that individual utilities should perform in conducting risk analyses and implementing solutions.

CHAPTER TWO: PRIVACY AND THE SMART GRID

Section 2.1. Any attempt to define Personally Identifiable Information (PII) must account for rules and definitions of PII in other jurisdictions. This document appears to be creating PII within this section. This section arguably is inappropriate and should merely suggest that utilities follow State guidelines on privacy. Where States have not defined privacy, it is incumbent upon utilities to provide definitions within their respective organizations and to work with state regulators to develop appropriate rules. There is also a difference between data privacy and data security. NIST should focus on data security issues, and especially upon data security that effectively frustrates security breaches that result in identity theft.

Section 2.4. “Areas of the electric system that cover the scope of a smart grid include the following:

the delivery infrastructure (e.g., transmission and distribution lines, transformers, switches), ... management of the generation and delivery infrastructure at the various levels of system coordination (e.g., transmission and distribution control centers, regional reliability coordination centers, national emergency response centers),”

In general, the transmission systems are already automated and operate as “smart systems.” The scope of Smart Grid should be limited to the automation of the distribution systems between the transmission system and the end use customer. If some entities contemplate further automation of their transmission infrastructure to support the deployment of a Smart Grid, existing standards should be utilized, not contradicted or inadvertently amended by these standards or any other new standards under development. If standards referring to transmission systems need to be revised to better support Smart Grid deployment in the distribution area, then the existing standards should be modified to include the necessary revisions. At the outset, it is critically important to recognize that cyber-security concerns at the transmission level differ significantly from those applicable to distribution systems.

Section 2.5. In Texas, individual usage data collected by smart meters is generally considered to be confidential and is owned by the customer. TEX. UTIL. CODE ANN. §§ 32.101(c) and 39.107(b) (Vernon 2009). In implementing these statutes, the Public Utility Commission of Texas (“PUCT”) has specifically identified “proprietary customer information” as meriting special protection. Pub. Util. Comm’n Subst. R. 25.272(c)(5) and 25.472(b)(1). Thus, the PUCT recognizes that there will be different security requirements for the use of operational data that is not PII.
Sec 2.5.3. It should be understood that advanced meters will collect the same customer usage data (registered in 15 minute increments), regardless of the type of retail electric service for which a consumer has contracted. As noted above, however, individual customer data is owned by the customer and cannot be distributed without prior customer consent. There are important exceptions to this principle. In Texas, there are generally four main entities that will receive the data: the TDU, the REP, the PUCT, and ERCOT. Sharing data with each of these entities is a precondition to receiving utility service because each entity performs essential “utility services.” For example, TDUs meter retail consumers’ electric usage and bill the various REPs serving individual consumers for T&D services and provide the detailed usage data to such REPs so that they can also bill the retail consumers for the electric services provided by each REP. The Electric Reliability Council of Texas has individual customer data as the independent system operator, but must keep such data confidential. Finally, the PUCT, of course, has the right to access such data as the governmental authority charged with regulation of electric utility service.

NIST should not alter the current carefully balanced structure of the Texas retail electric market concerning access to individual customer usage data, which might be inferred from the discussion in Section 2.5.3. Texas maintains a carefully structured set of laws and regulations concerning the protection of such data. The Company is concerned that certain requirements proposed in the Draft Report may frustrate the balance of this structure, which has proven to be very effective.

Section 2.5.6. Currently, customer information that is held confidential and is owned by the customer, like kWh usage data, is stored for specific purposes, like billing, and will be made available to the consumer upon request. The consumer is not, however, given access to the data in every system in which it is stored. Granting such access would create an unnecessary and unreasonable security risk, since the data is stored in secure systems within the utility.

**CHAPTER FOUR: AMI SECURITY REQUIREMENTS**

The Company’s initial comments on Chapter Four are divided into four categories based on the nature and existence of available technology: (i) requirements that involve currently evolving technology; (ii) requirements where technology exists yet CEHE is using alternate methods to address; (iii) requirements where no current technology exists to satisfy; and (iv) requirements that are not clear and need further detail.

(i) **Requirements that involve currently evolving technology**

The NIST requirements below fall into the category of currently evolving technology. After reviewing the requirements below, CEHE understands that they will be met in its system over the next two to five years. The components that make up the AMI system are not mature, and the vendors who manufacture this equipment are continuously working to include new security enhancements in future releases of their products. The NIST requirements, however, should be refined to remove statements requiring “all components” to include security features. Many security requirements can effectively be handled in a central “system” method.

In many of the requirements listed below, the document states that meeting the requirement is “problematic” in an AMI component. In these cases, products must become commercially

-6.
available and technological solutions must be developed before the requirement should be enforceable. **DHS 2.8.3 Security function Isolation** (specifically DHS 2.8.3.1), **DHS 2.8.5 Denial of Service Protection** (specifically DHS 2.8.5.1, DHS 2.8.5.2), **DHS Boundary Protection** (specifically DHS 2.8.7.1, DHS 2.8.7.2), **DHS 2.8.11 Cryptographic Key Establishment and Management**, **DHS 2.8.14 Transmission of Security Parameters** (specifically DHS 2.8.14.1), **DHS 2.10.9 Remote Maintenance** (specifically DHS 2.10.9.1), **DHS 2.12.8 Incident Monitoring** (specifically DHS 2.12.8.3), **DHS 2.14.4 Malicious Code Protection** (All), **DHS 2.14.7 Software and Information Integrity** (specifically DHS 2.14.7.1), **DHS 2.14.10 Information Input Accuracy, Completeness, Validity, and Authenticity (All)**, **DHS 2.14.11 Error Handling** (All), **DHS 2.15.18 Concurrent Session Control** (All), **DHS 2.15.20 Unsuccessful Login Attempts** (All), **DHS 2.15.21 Session Lock** (All), **DHS 2.15.22 Remote Session Termination** (All), **DHS 2.15.30 Unauthorized Reporting** (All), **DHS 2.16.2 Auditable Events** (specifically DHS 2.16.2.1), **DHS 2.16.3 Content of Audit Records** (specifically DHS 2.16.3.1), **DHS 2.16.4 Audit Storage Capacity** (All), **DHS 2.16.8 Time Stamps** (All).

(ii) **Requirements where technology exists yet CEHE is using alternate methods to address**

The requirements for **SPAM Protection** (DHS 2.14.8 All), and **Access Control** (DHS 2.15 All), need to be flexible enough to allow for enterprise class systems. Alternative effective methods of providing these controls should be allowed to meet the requirement. All AMI systems do not require segregation from IT enterprise system management. Enterprise email gateway “SPAM” protection and enterprise identity management systems are more effective than distributed solutions. Furthermore, distributed solutions require installation on endpoint components, version and configuration control, and constant monitoring. In general, the requirements need to be more flexible to allow alternatives that meet the security requirement for efficiency and effectiveness.

(iii) **Requirements where no current technology exists to satisfy**

Technology to meet the requirements for **Malicious Code Protection** as described in **DHS 2.14.3.1, DHS 2.14.3.3** does not exist in current meter and HAN end point devices. Furthermore, adding such functionality to these devices could drive the cost of the devices out of the consumer price range and hinder consumer adoption of the technology. NIST states that “field deployed host devices are typically not suitable for traditional third party host based malicious code protection mechanisms.” The requirements in this area need to be flexible enough to allow for reasonable malicious code protections at central points within the AMI system and not on every component.

(iv) **Requirements that are not clear and need further detail**

The requirements listed below need further clarification for AMI implementers to be able to evaluate the impact to the current and planned implementation. It is not clear what is being recommended here and what the requirements will be. **DHS 2.8.17 Voice Over Internet Protocol** (All), **DHS 2.8.20 Message Authenticity** (All), **DHS 2.8.21 Architecture for**
Provisioning Name/Address Resolution (All), DHS 2.8.22 Secure Name/Address Resolution Service (All), DHS 2.12.18 Fail-Safe Response (All).

Conclusion

The Company reiterates its appreciation for the opportunity to comment on NIST’s Draft Report and thanks NIST for its efforts in helping to secure the Smart Grid. In sum, CEHE believes that a balanced cyber security program—based on performance standards and focused on flexibility—is of paramount importance to its viability and effectiveness. The Company also urges NIST to pay particularly close attention to the unique nature of the Texas electric retail market and how it interacts with CEHE (as opposed to some other utilities). It is this unique relationship that is the basis for many of CEHE’s comments, especially those that relate to the benefits of enabling local markets to enforce any regulations, standards, or requirements that the Federal government believes is necessary to secure the Smart Grid.

Date: November 24, 2009

Respectfully submitted,

Kenneth M. Mercado, Sr. Division Vice President  
Advanced Metering System Deployment  
CenterPoint Energy Houston Electric, LLC  
1111 Louisiana Street  
Houston, Texas 77002  
(713)207-3200