

**BEFORE THE PUBLIC UTILITIES COMMISSION OF  
THE STATE OF OHIO**

IN THE MATTER OF THE REVIEW OF THE  
CONSUMER PRIVACY PROTECTION,  
CUSTOMER DATA ACCESS, AND CYBER  
SECURITY ISSUES ASSOCIATED WITH  
DISTRIBUTION UTILITY ADVANCED  
METERING AND SMART GRID  
PROGRAMS

CASE NO. 11-277-GE-UNC

**COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

The Telecommunications Industry Association (“TIA”) is pleased to provide comments in response to the Commission’s inquiry regarding smart grid privacy and data access issues. TIA is the leading trade association for the Information and Communications Technology (“ICT”) industry. With 500 member companies that manufacture or supply the ICT products and services that will make the smart grid a reality, TIA is committed to the successful and secure modernization of the electric grid in a way that ensures privacy of consumer data without sacrificing innovation of smart grid technology.

**TIA COMMENTS**

Electric utilities and the ICT industry share a long tradition of partnering to build and maintain the communications networks contributing to the security and reliability of the grid. Advances in technology and more robust use of ICT to transform the current electric grid into a smart grid present exciting opportunities for consumers and utilities in the State of Ohio and throughout the United States. While the potential benefits of a smart grid are clear, at this nascent stage in its development, the policy and regulatory framework in which the grid matures will

significantly impact how smart the grid can become and the benefits it can achieve in both the short and long term. TIA appreciates the leadership position that the Commission is taking and appreciates the opportunity to share our perspective.

As smart grid deployments move forward in the State of Ohio, the Commission will need to consider, develop, and adopt additional policies related to privacy and data access to consumer energy usage data in order to appropriately fit regulation to what smart grid technologies make possible. As the Commission is aware, several other states are examining data access and privacy issues as they relate to smart grid deployments and many more will be considering these issues in the near future. State-by-state regulations and requirements related to data access will have implications on both the development and deployment of smart grid technologies. TIA recommends that the Commission takes into consideration work being done at the federal level, such as in the NIST Smart Grid Interoperability Panel, and in other states and work toward uniform policies and a common market for smart grid technologies.

TIA recommends consideration of the following issues:

### **CONSUMER & THIRD PARTY DATA ACCESS**

#### **PROVIDE CONSUMERS ACCESS TO USAGE, PRICING AND CARBON-MIX DATA IN MACHINE-READABLE FORM FOR USE IN THIRD-PARTY APPLICATIONS**

While consumer preferences for both the manner and the amount of interaction with the grid will vary significantly by individual, the secure provision of energy consumption data to customers, utilities and third parties will be critical to the development of the smart grid.

Consumers and utilities share a dual-ownership role with regard to the right to access customer energy consumption data. Customers should have a right to access consumption data in real time or near real time to both monitor and manage energy usage. Utilities should have a right to access consumption data necessary for management of the electric grid and billing purposes.

Third-party service providers will play a role in providing competition and innovation in consumer home energy management services. In addition to accessing the data themselves, consumers need the ability to authorize access to that data in real time or near real time to third-party service providers. Whether the data is generated by customer-installed sensors or by the utility provider, customers should maintain control over which third parties are authorized to access personal billing and energy consumption information. TIA recommends where possible that the Commission work with other states and federal policymakers to develop a uniform national policy to avoid fracturing the market with patchwork regulation and requirements.

### **PROVIDE CONSUMERS WITH UNIFORM AND CONSISTENT PRIVACY POLICIES**

Uniform and consistent privacy policies will be critical to protect consumer information. TIA believes Fair Information Practice Principles (FIPPs) as provided by the U.S. Federal Trade Commission should serve as the basis for developing policies regarding the privacy of energy consumption information. In developing specific policies and practices for energy data, the Commission should examine policies and self-regulatory models from other sectors that rely on both technology and strict procedures to protect critical data. The privacy framework for the smart grid should protect privacy without sacrificing innovation. In taking a comprehensive and in-depth look at smart grid privacy, the Privacy Subgroup of the Cybersecurity Coordination Task Group at NIST has published NIST IR-7628, which outlines their relevant findings and provides a broad framework for the privacy of smart grid data.<sup>1</sup> As a general rule, TIA believes customer authorization should be the prerequisite for releasing data to a third party. As with data access requirements, TIA recommends that the Commission coordinate with other states and federal policymakers with the goal of working towards a uniform national policy.

---

<sup>1</sup> See NIST Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid (August 2010), available at [http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=906224](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=906224).

## **ADDITIONAL CONSIDERATIONS**

TIA recommends that the Commission also take into account the importance of technology neutrality, voluntary standards and cybersecurity in providing consumers with private and secure access to data.

## **TECHNOLOGY NEUTRALITY ACROSS AN OPEN SMART GRID ARCHITECTURE IS CRITICAL FOR INNOVATION OF SMART GRID SOLUTIONS**

At this early stage, it is impossible to predict which technology or combination of technologies will ultimately be the most successful. TIA recommends that federal and state governments, through either the policy-making, regulatory or standards-setting process, avoid excluding viable technologies or architectures and instead focus on the coexistence and interoperability of a group of viable technologies. Regulatory requirements specific to technology requirements or architectures used in a deployment should be flexible and informational rather than rigid and prescriptive. As we have seen at the early stages of other developing technologies, technology neutrality is critical to create an ecosystem of competition and innovation. From a technology perspective, deployment plans will need to be flexible as utilities continue to adopt and integrate new solutions as they become available. Technology neutrality will lead to increased innovation in smart grid technologies and increased options for a range of customer needs and preferences, and provide a reliable and secure grid that reduces energy consumption and costs for consumers. Allowing multiple technologies to compete to achieve the goals of a smart grid will increase investment in the market, spur more innovation in products and solutions, and future proof the grid, allowing it to realize its potential. An open architecture where multiple interoperable technologies can coexist and compete is the most beneficial approach both for consumers and for the development and deployment of the smart

grid in the short and long term. Smart grid deployment plan requirements will need to provide adequate flexibility for utilities to adopt and integrate new solutions as they become available.

**ALLOW FOR VOLUNTARY STANDARDS TO SUPPORT THE DYNAMIC NATURE OF ICT INNOVATION AND TO MAXIMIZE FLEXIBILITY AND CHOICE IN A RAPIDLY CHANGING, MARKET-DRIVEN ECOSYSTEM**

Nowhere is the principle of technology neutrality more important to the development of the smart grid than in the standards development and identification process being coordinated by NIST. Alternative architectures could include a variety of combinations of smart meters, home energy management systems, Internet-based energy management services and other methods to support ongoing innovation. At this stage, technology neutrality, flexibility in standard-setting and reliance on voluntary standards are key to the development of the smart grid. Standards are important tools to promote efficiency, interoperability and innovation by making products and services work together better. By helping to enhance interoperability among products and services within a market and by being responsive to real marketplace needs, standards can help promote innovation, fuel market growth, protect investment in new technologies and bring down costs. However, standards are only a means to an end. They are useful tools if they are effective at addressing a real marketplace need.

Given the dynamic nature of innovation and ICT standards development, governments should be cautious about mandating adherence to any particular standard without demonstrating sufficient need and without support from impacted industry and relevant stakeholders. Mandated standards can disrupt normal marketplace outcomes and discourage competition. In addition, identifying a single standard that is appropriate for all circumstances is extremely difficult, if not impossible. The breadth and depth of the ICT environment means that there is rarely, if ever, a one-size-fits-all solution. Moreover, because the world of technology typically moves at a far

greater pace than the policy-making, regulatory and legislative processes, it is quite possible for a government to mandate a standard that becomes irrelevant in the marketplace over time.

Standards do best as part of an active, competitive habitat. For governments that want to foster innovation in their technology sectors, it is vital to encourage new technologies, valuable intellectual property, improved human capital, venture investments, and economic growth.

Mandating distinct standards potentially dampens incentives to innovate in a technology area and can have adverse effects on both economic and social outcomes.

While standards can promote interoperability, they do not guarantee it. Standards can best support interoperability when they are part of a multi-faceted approach incorporating open standards-setting processes, proactive standards maintenance and a strong effort to ensure that different implementations of the same standard will in fact interoperate.

Under NIST Special Publication 1108 (the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0), some of the “Guiding Principles for Identifying Standards for Implementation” include whether the standard:

- Is well-established and widely acknowledged as important to the smart grid.
- Is an open, stable and mature industry-level standard developed in consensus processes from a standards development organization (SDO).
- Has, or is expected to have, significant implementations, adoption, and use.
- Is supported by an SDO or Users Group to ensure that it is regularly revised and improved to meet changing requirements and that there is strategy for continued relevance.

Before mandating adherence to any standard recommended by NIST and the Smart Grid Interoperability Panel, regulators should first consider whether the standard is in fact likely to be widely implemented by stakeholders on a voluntary basis. In that situation, regulators should consider recommending such standards instead of including them in a regulatory framework in order to preserve further innovation and competition in the marketplace and the opportunity to

make further improvements to the standard over time in response to perceived needs for improvements.

TIA recommends that the Commission should defer adoption of standards until NIST has progressed in identifying smart grid standards and protocols. Adoption of standards and protocols at the state level is premature, given the ongoing status of the NIST process. The ICT industry is actively engaged with the NIST in helping them fulfill their responsibility of coordinating standards and protocols for the interoperability of smart grid solutions. After the NIST process has progressed, TIA recommends that state regulators then evaluate any additional issues involving standards or protocols that they will need to address beyond the NIST process.

#### **POLICYMAKERS SHOULD SEEK TECHNICAL EXPERTISE FROM QUALIFIED AND NEUTRAL THIRD PARTIES IN DECISIONS RELATING TO CYBERSECURITY**

By addressing cybersecurity early in the process, smart grid stakeholders can benefit by instituting optimal security policies and principles prior to the deployment of new technologies. Cybersecurity requires good security processes up front and ongoing management to mitigate current and emerging threats. Utility regulators can benefit from best practices developed in other industries, such as finance, information technology and healthcare, that rely on ICT to protect assets and information. On technical matters, TIA encourages policymakers and utility regulators to seek the opinion of qualified neutral third parties when evaluating and rendering smart grid decisions that involve ICT, as well as looking to established guidelines such as those provided by NIST. The convergence of ICT and energy services represents a major transformation of our energy infrastructure, and TIA believes consumers would be best served if the capabilities of ICT are well understood by regulators and leveraged where appropriate. In particular, the technical aspects of securing smart grid and smart meter communications and

protecting customer data are highly complex. Smart grid decisions based on inadequate information may result in systems containing vulnerabilities that negatively impact the reliability of energy services, the privacy of consumers, and the ability of the smart grid to deliver its full potential. It may further result in undesirable post-deployment costs to remediate security shortcomings that could have been avoided through an independent information security assessment during the planning stage and the use of proven secure development and deployment processes. There are several qualified sources of important information about security and privacy best practices in the government and private sector that can assist in evaluating the security of a proposed implementation. The Commission should provide adequate funding to enable utilities to acquire the necessary resources to build robust cybersecurity into their networks. State regulators should coordinate efforts in communicating best practices for cybersecurity.

## **CONCLUSION**

TIA appreciates the opportunity to file these comments and looks forward to working with the Commission and partnering with other stakeholders on these issues.

Respectfully submitted

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

/s/ DANIELLE COFFEY

Danielle Coffey  
Vice President,  
Government Affairs

Joseph Andersen  
Advisor  
Telecommunications Industry Association  
10 G Street NE, Suite 550  
Washington, DC 20002  
Tel: (202) 346-3249  
Fax: (202) 346-3241  
jandersen@tiaonline.org

March 4, 2011