UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY

Smart Grid RFI: Addressing Policy and Logistical Challenges

The National Association of Regulatory Utility Commissioners (NARUC) appreciates the opportunity to provide comments to the Department of Energy (DOE) on this Request for Information (RFI) regarding the policy and logistical challenges of the smart grid. 75 Fed. Reg. 57006 (Sept. 17, 2010).

INTRODUCTION

NARUC is the national organization of State commissions responsible for economic and safety regulation of utilities. Our members in the fifty States, the District of Columbia, Puerto Rico, and the Virgin Islands have the obligation under State law to ensure the establishment and maintenance of such energy utility services as may be required by the public convenience and necessity, as well as ensuring such services are provided at just and reasonable rates. NARUC members have been wrestling for some time with many issues raised in the RFI.

We appreciate DOE's recognition that State regulators play a both a critical and an essential role to ensure cost effective smart grid deployments can be implemented successfully in individual States and regions.

COMMENTS

Although individual commissions must evaluate specific utility deployment proposals to assure the record justifies the investment, NARUC generally supports the adoption and implementation of smart grid technology. Smart upgrades to the transmission and distribution system often provide clear and quantifiable benefits that can make the grid more efficient, reliable, and less expensive.

End-user focused technologies also have the potential to allow educated consumers to take more control over their energy usage. Like any new technology, though, the promise of these new technologies must not preclude a careful examination and balancing of the costs and benefits of specific utility technology, rate design/cost recovery, consumer education, security, and deployment proposals. The integration of each new technology into the grid, particularly "smart meters," must be carefully considered to assure the investments of ratepayer dollars are prudent, the benefits are clear, and consumers are protected. State commissions play the central and critical role in ensuring that outcome.

The provisions of the Energy Independence and Security Act of 2007, as well as the billions of federal dollars dedicated to smart grid projects in the American Recovery and Reinvestment Act of 2009 demonstrate that increasing the intelligence of the grid at all levels is a federal priority. Both respect the critical role State regulators play in the context of this broad federal vision. With a strong and cooperative State-federal relationship, creating a workable, reliable, and economically efficient smarter grid is possible.

NARUC welcomes the opportunity to work, through our Smart Grid Working Group, with the Smart Grid Subcommittee of the National Science and Technology's Committee on Technology in three areas: Technical Assistance to the States, Consumer Engagement and Education, and Technology Learning Labs. All three initiatives promise to enhance State commissions' ability to evaluate smart grid proposals and make the best possible decisions. Obviously, assistance must be tailored to support States' sound decision-making processes and the creation of accurate and complete factual records, not any particular end result.

States make decisions in a deliberative, record based process where utility commissioners evaluate evidence and determine the best course forward in the context of the

local or regional infrastructures and regulatory paradigms. The only smart approach is to craft the collaboration to fit States' needs. As noted earlier, the focus should be to support States' review processes to facilitate sound, but not pre-ordained, decisions on particular utility proposals that are justified by record evidence. A clearinghouse dedicated and designed to assist State regulators that gathers data from pilots and other previously approved projects and provides analysis of successful and unsuccessful deployments could be helpful.

NARUC creates association-wide policy through resolutions. The association has approved three resolutions on Smart Grid. They are attached. As Congress and the White House address smart-grid issues, NARUC's resolution specifically endorses the following principles to guide policy development.

Specifically, smart grid standards and federal policy should:

- Enhance interoperability consistent with ensuring cybersecurity and maintaining or improving reliability;

- Understand that the development of smart grid standards can best be achieved through a partnership among the States, the federal government, and industry. State regulatory commissions play an essential role in evaluating smart grid deployments; early deployments will influence the emergence of de facto and de jure standards;

- Seek to achieve maximum consumer, reliability, and environmental benefits and to provide opportunities for innovation, consistent with providing utility service to consumers at fair, just, and reasonable rates.

- Recognize the inherent value within the State regulatory process and the manner in which it balances the needs of the utilities, the grid system, and consumers;

- Recognize that State commissions have jurisdiction over the elements of smart grid improvements within their vested authority; FERC should not authorize cost recovery for smart grid investments that are within the State commissions' jurisdiction; FERC and the State commissions must prohibit double cost-recovery for the same investment;

- Create standards that should enable a common semantic framework and provide for cyber secure interoperable communications through open protocols and standards (including Internet-based protocols and standards) if available and appropriate;

- Be flexible and together with RTO policies and tariffs, should accommodate various State regulatory contexts, retail rate structures, and policy goals.

- Promote a flexible, non-proprietary, open infrastructure that is upgradeable to avoid excess costs as a result of obsolescence;

- Balance the costs of the smart grid with the benefits of the smart grid and the costs and benefits should be quantified to the extent possible;

- Provide consumers with protections that ensure the privacy of customer information while allowing for the benefits the deployment of the smart grid promises;

- State commissions should take steps to ensure that their regulated utilities make cost-effective decisions that safeguard customers' privacy and that authorized third parties have responsibilities to protect this information and the privacy of customers; and

- Respect and incorporate State rules and ongoing State authority to protect ratepayers' privacy and ability to control access to their energy usage information.

More often than not, NARUC's member State commissions have been at the cutting edge of deploying new technologies and regulatory schemes. We frequently pass resolutions to assist members on new issues. The remaining two resolutions are advice directed, not at federal authorities, but our State brethren. Still they contain useful principles than anyone interested in grid modernization should consider on cybersecurity and advanced meter deployment. The second NARUC resolution recognizes the need for continued vigilance against all potential sources of cyber threats and encourages member commissions to:

- Be both prepared to prevent cyber attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety, and the economy;

- Make efforts to give the highest priority to ensure that cybersecurity will be consistently monitored and evaluated to remain effective to meet ongoing threats to the utility systems in collaboration with those agencies having expertise in cyber-threat management and mitigation;

- Open a dialogue with their regulated utilities to ensure that these organizations are in compliance with standards, and where applicable, ensure that cost-effective protection and preparedness measures are employed to deter, detect, and response to cyber attacks, and to mitigate and recover from their effects;

- Supports member PUCs to become and remain more knowledgeable about these threats, and ensuring that their own staffs have the capability, training, and access to resources to adequately review and understand cybersecurity issues that enhances expertise in the review of cybersecurity aspects of filings by their jurisdictional utilities; and

- To regulatory revisit their own cybersecurity policies and procedures to ensure that they are in compliance with applicable standards and best practices, such as those of the National Institute of Standards and Technology (NIST) and Certification for Information System Security Professionals (CISSP).

The last NARUC resolution on smart grid issues is also directed at its members. That resolution both (1) recognizes the benefits that advanced metering infrastructure (AMI) brings to the smart grid – including but not limited to – providing greater customer control over consumption and electric bills and improved metering accuracy, and (2) recommends that commissions seeking to facilitate the deployment of cost-effective AMI technologies consider the following regulatory options:

- Pursue an AMI business case analysis, in conjunction with each regulated utility, in order to identify an optimal, cost-effective strategy for deployment of AMI that takes into account both tangible and intangible benefits;

- Adopt ratemaking policies that provide utilities with appropriate incentives for reliance upon demand-side resources;

- Provide for timely cost recovery of prudently incurred AMI expenditures, including accelerated recovery of investment in existing metering infrastructure, in order to provide cash flow to help finance new AMI deployment; and

- Provide depreciation lives for AMI that take into account the speed and nature of change in metering technology.

RESPECTFULLY SUBMITTED:

JAMES BRADFORD RAMSAY
General Counsel

ROBIN J. LUNT
Assistant General Counsel

National Association of Regulatory Utility Commissioners
1101 Vermont Ave, NW
Suite 200
Washington, DC 20005

November 1, 2010

ATTACHMENTS

Resolution Regarding Smart Grid

WHEREAS, The Energy and Independence and Security Act of 2007 (EISA) establishes as policy the demonstration and deployment of a smart grid; *and*

WHEREAS, The American Recovery and Reinvestment Act of 2009 provided funds to support these smart grid initiatives; *and*

WHEREAS, The Federal Energy Regulatory Commission (FERC) issued a Smart Grid policy statement prioritizing the National Institute of Standards and Technology's (NIST) development of smart grid interoperability standards (as mandated in EISA); FERC encourages the development of interoperability standards consistent with cyber security and reliability standards in four prioritized functionalities (wide-area situational awareness, demand response, electric storage, and electric transportation); FERC's policy statement established an interim rate policy for smart grid investments; and the areas highlighted by FERC's policy statement overlap with State commissions' jurisdiction; *and*

WHEREAS, The White House, Department of Commerce, and the Department of Energy have repeatedly stated that the Administration considers the smart grid an essential element of America's job growth, energy independence, and future as a global economic leader, and emphasized the urgency of developing smart grid standards; *and*

WHEREAS, The Department of Energy has released funding opportunity announcements for smart grid investment grants and demonstration projects that will spur investment in smart grid, and require applicants to provide at least 50% cost share for any selected project, which cost share might be recovered through utility rates; *and*

WHEREAS, Various States and commissions are pursuing smart grid projects and deployment according to the needs and interests of their constituents; *now, therefore be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its 2009 Summer Committee Meetings in Seattle, Washington, recognizes the smart grid's potential to revolutionize the nation's energy grid; *and be it further*

RESOLVED, That NARUC agrees that to be most effective, the federal policies and standards that guide the deployment of the smart grid should be based on the following principles:

1. Smart grid policies and standards should enhance interoperability consistent with ensuring cyber security and maintaining or improving reliability.
2. The development of smart grid standards can best be achieved through a partnership among the States, the federal government, and industry. State commissions play an essential role in evaluating smart grid deployments; early deployments will influence the emergence of de facto and de jure standards.
3. Smart grid standards and policies should seek to achieve maximum consumer, reliability, and environmental benefits and to provide opportunities for innovation, consistent with providing utility service to consumers at fair, just, and reasonable rates.

4. There is inherent value within the State regulatory process and the manner in which it balances the needs of the utilities, the grid system, and consumers.
5. State commissions have jurisdiction over the elements of smart grid improvements that are within their vested authority; FERC should not authorize cost recovery for smart grid investments that are within the State commissions' jurisdiction; FERC and the State commissions must prohibit double cost recovery for the same investment.
6. Smart grid standards should enable a common semantic framework and provide for cyber secure interoperable communications through open protocols and standards (including Internet-based protocols and standards) if available and appropriate.
7. Smart grid policies and standards should be flexible and together with RTO policies and tariffs, should accommodate various State regulatory contexts, retail rate structures, and policy goals.
8. Smart grid policies and standards should promote a flexible, non-proprietary, open infrastructure that is upgradable to avoid excess costs as a result of obsolescence.
9. Smart grid policies should encourage interoperability of the electric grid and information services to foster a vast array of resources and information services.
10. Smart grid policies and standards should balance the costs of the smart grid with the benefits of the smart grid and the costs and benefits should be quantified to the extent possible.

Sponsored by the Committees on Electricity, Energy Resources and the Environment, and Critical Infrastructure
Adopted by the NARUC Board of Directors July 22, 2009

Resolution on Smart Grid

WHEREAS, Smart grid deployment can help bring our electrical grid into the 21st century by enabling the more efficient, reliable and affordable consumption of electricity and allow third party providers of energy services access to consumer information which may spur innovation and economic development; *and*

WHEREAS, The National Association of Regulatory Utility Commissioners (NARUC) adopted a resolution in July 2009 sponsored by the Committees on Electricity, Energy Resources and the Environment, and Critical Infrastructure calling for, among other things, policies and standards that "should promote a flexible, non-proprietary, open infrastructure," and "encourage interoperability of the electric grid and information services to foster a vast array of resources and information services;" *and*

WHEREAS, The Federal Communications Commission (FCC) in its March 2010 National Broadband Plan, stated that "[A] national Smart Grid policy should encourage tens of thousands of entrepreneurs to innovate – using new technologies and business models – to create a wide variety of in-building energy management and information services" and that "[M]aking energy data available to customers and their authorized third parties, while employing open and non-proprietary standards, is the best way to unleash this vast potential for innovation;" *and*

WHEREAS, The FCC recommended that "[S]tates should require electric utilities to provide consumers access to, and control of, their own digital energy information, including real-time information from smart meters and historical consumption, price and bill data over the Internet; *and*

WHEREAS, While the deployment of smart grid technologies may empower the consumer and provide more options, it also poses significant privacy issues that need to be considered and resolved by regulators; *and*

WHEREAS, Control of the smart grid network and the proper roles and responsibilities of electric utilities, telecommunication companies, and others are still being determined; *and*

WHEREAS, Because traditionally, privacy regulation usage data has been a State responsibility, consumers already turn to their State commissions for service and billing disputes; *and*

WHEREAS, The United States Department of Energy has recognized the need to balance the benefits of data collection with the protection of personal privacy; *and*

WHEREAS, Smart grid deployments will utilize various wired and wireless communications technologies over utility-owned and commercial communications networks to transmit data, that will include sensitive customer information and energy consumption data; *and*

WHEREAS, It is crucial that State-approved smart grid technology deployment plans continue to be subject to a record-based review by States to ensure proposals – and in particular – the

utility's proposal for recovery of its capital outlays, are both cost-effective and actually result in benefits to ratepayers; *and*

WHEREAS, The adoption of the smart grid will allow for the collection of specific information about individual customer electric use, including individual end-use applications, and electric bill payment data; *and*

WHEREAS, Most States and electric utilities have policies to protect customer energy usage data (CEUD) with the premise that such information be kept confidential absent customer authorization for its release; *and*

WHEREAS, Information on the operation, reliability, and safety of the electric systems must remain secure; *and*

WHEREAS, Third parties entering the market may seek access to customers and utility data, *now, therefore be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its 2010 Summer Committee Meetings in Sacramento, California, recognizes the need to provide consumers with protections that ensure the privacy of customer information while allowing for the benefits the deployment of the smart grid promises; *and be it further*

RESOLVED, That NARUC encourages the National Regulatory Research Institute to expeditiously complete its study addressing consumer and operational data guidelines for States to consider when implementing smart grid technologies; *and be it further*

RESOLVED, That the State regulatory commissions, which have the responsibility for ensuring reasonable rates for local utility service, take steps to provide that utilities, subject to State commission oversight, make cost-effective decisions while at the same time safeguarding their customers' privacy and that authorized third parties have responsibilities to protect this information and the privacy of customers; *and be it further*

RESOLVED, That any Congressional or federal agency action should respect and incorporate State rules and ongoing State authority to protect ratepayers' privacy and ability to control access to their energy usage information; *and be it further*

RESOLVED, That NARUC make every effort to give the highest priority to ensure that consumers are protected as the smart grid evolves.

Sponsored by the Committees on Telecommunications and
Energy Resources and the Environment
Adopted by the NARUC Board of Directors July 21, 2010

Resolution Regarding Cybersecurity

WHEREAS, The National Infrastructure Protection Plan (NIPP) identifies Energy, Communications, and Water as interdependent national critical infrastructures; *and*

WHEREAS, Extended interruption to reliable utility service has cascading secondary impacts capable of causing significant harm to public health, public safety, and the economy; *and*

WHEREAS, Threats to critical utility infrastructure from all extraordinary events, natural or man-made, have the potential to interrupt reliable utility service; *and*

WHEREAS, Man-made threats can take the form of attacks on both physical and cyber assets; *and*

WHEREAS, Cyber attacks may be undertaken to infiltrate the control systems which operate and maintain our most critical utility infrastructure including Supervisory Control and Data Acquisition systems (SCADA) which regulate our water and wastewater treatment and distribution, transmission and distribution of electricity and natural gas, and communication networks for the very purpose of causing disruption or harm to public health, public safety, government, and the economy; *and*

WHEREAS, Threats to control-systems through breaches of cyber security may be initiated by any number of sources including but not limited to hackers, disgruntled current or former employees, criminal enterprises, terrorists, and foreign governments; *and*

WHEREAS, Threat of cyber attack against control systems cannot be eliminated but actions can be taken to reduce the likelihood of a successful attacks, to mitigate the harmful consequences of an attack, and to improve a utility's ability to improve system protection and restoration from future attacks, and thus enhance the resiliency of critical utility systems; *and*

WHEREAS, Measures to prevent an attack or mitigate its consequences come with costs which must be balanced against the likelihood of the threat and the significance of the potential harm; *and*

WHEREAS, Recognized industry-specific standards exist which identify protocols for protection from the threat of cyber attack on critical electric, gas, telecommunications, and water infrastructures; *and*

WHEREAS, Federal Energy Regulatory Commission (FERC) Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection, issued on January 8, 2008, approves eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to FERC by the North American Electric Reliability Corporation (NERC) which require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets; *and*

WHEREAS, The U.S. Department of Energy (DOE) has designated NERC as the electricity sector coordinator for critical infrastructure protection; *and*

WHEREAS, NERC has constituted a Critical Infrastructure Protection Program to coordinate all NERC efforts to improve both physical and cyber security, including standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues; *and*

WHEREAS, the U.S. Department of Commerce and National Institute of Standards and Technology (NIST) have issued a report on Smart Grid Cyber Security Strategy and Requirements that provides the NIST Smart Grid Cyber Security Coordination Task Group's overall cyber security strategy for the Smart Grid; *and*

WHEREAS, The gas industry largely relies upon the Security Practices Guidelines developed by the U.S. Department of Transportation's Office of Pipeline Safety[1] and the U.S. Department of Homeland Security's Transportation Security Administration; *and*

WHEREAS, The Network Reliability and Interoperability Council (NRIC) in collaboration with the Federal Communication Commission (FCC) maintains a repository of Best Practices[2] for the telecommunications industry; *and*

WHEREAS, The U.S. Environmental Protection Agency (EPA) oversees cyber protection efforts for the drinking water industry through mandated vulnerability assessments and support training for emergency response to threats from breaches of cyber security; *and*

WHEREAS, The threshold for measuring cyber security is unclear and industry compliance standards are constantly changing to meet the threats of cyber-attacks, making it increasingly difficult to ensure cyber-secure systems; *now, therefore be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its 2010 Winter Committee Meetings in Washington, D.C., recognizes the need for continued vigilance against all potential sources of cyber threat to be both prepared to prevent cyber attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety, and the economy; *and be it further*

RESOLVED, That NARUC encourages commissions to make efforts to give the highest priority to ensure that cyber security will be consistently monitored and evaluated to remain effective to meet ongoing threats to the utility systems in collaboration with those agencies having expertise in cyber threat management and mitigation; *and be it further*

---

[1] "The Role of State Public Utility Commissions in Protecting the National Utility Infrastructure: Cost Recovery, Sensitive Information, and Security Guidelines," NRRI Briefing Paper (March 2005).

[2] See https://www.fcc.gov/nors/outage/bestpractice/ProcessBestPractice.cfm?RequestTimeout=500

RESOLVED, That NARUC encourages commissions to open a dialogue with their regulated utilities to ensure that these organizations are in compliance with standards, and where applicable, ensure that cost-effective protection and preparedness measures are employed to deter, detect, and respond to cyber attacks, and to mitigate and recover from their effects; *and be it further*

RESOLVED, That NARUC supports member commissions in becoming and remaining knowledgeable about these threats, and ensuring that their own staffs have the capability, training, and access to resources to adequately review and understand cyber security issues that enhances expertise in the review of cyber security aspects of filings by their jurisdictional utilities; *and be it further*

RESOLVED, That NARUC encourages commissions to regularly revisit their own cyber security policies and procedures to ensure that they are in compliance with applicable standards and best practices, such as those of the National Institute of Standards and Technology (NIST) and Certification for Information System Security Professionals (CISSP).

Sponsored by the Committees on Critical Infrastructure, Electricity, Telecommunications, and Gas
Adopted by the NARUC Board of Directors, February 17, 2010