Power to Ontario.
On Demand.

Independent Electricity
System Operator
655 Bay Street
Suite 410, PO Box 1
Toronto, Ontario M5G 2K4
t 416 506 2800

www.ieso.ca

**BY RESS & COURIER**

April 20, 2012

Ms. Kirsten Walli
Board Secretary
Ontario Energy Board
P.O. Box 2319
2300 Yonge Street, 27th Floor
Toronto, ON, M4P 1E4

Dear Ms. Walli:

**Re: Independent Electricity System Operator Submissions on Staff Discussion Paper on the Establishment, Implementation and Promotion of Smart Grid in Ontario – Renewed Regulatory Framework for Electricity – EB -2011-0004**

The Independent Electricity System Operator (the "IESO") provides this submission in response to the Ontario Energy Board's (the "OEB") request for stakeholder comments in regard to the Renewed Regulatory Framework for Electricity, and in particular, the OEB's staff discussion paper, "*In regard to the Establishment, Implementation and Promotion of Smart Grid in Ontario*" (EB-2011-0004). The IESO's interest in this consultation is threefold:

1) The IESO is the operator of the province's Bulk Electricity System (the "IESO-controlled grid") and the wholesale market for electricity (the "IESO-administered markets"). Various technological and commercial developments arising from the evolution of the Smart Grid may pose challenges to the IESO, yet also provide opportunities to better serve the changing needs of customers and the broader electricity sector.

2) As the facilitator of the Ontario Smart Grid Forum (the "Forum"), the IESO sees a strong connection between many of the directional recommendations of the Forum and topics

raised in the OEB's staff discussion paper. In particular, the May 2011 report of the Smart Grid Forum, "*Modernizing Ontario's Electricity System: Next Steps"* makes several recommendations related to various Key Issue Areas identified by OEB staff – particularly those pertaining to "behind the meter" (BTM) services. The technical working group of the Forum and its Corporate Partners Committee of private sector companies are also examining various aspects of BTM services, and the interaction between Local Distribution Companies and customer home area networks. The Forum has also been influential in proposing high-level Smart Grid principles which now form the basis of the Ontario Energy Minister's November 23, 2010 Smart Grid directive to the OEB, which is cited at the outset of the staff discussion paper.

(None of the comments in this submission should be viewed as those of the Smart Grid Forum, as individual member organizations of the Forum may make their own submissions.)

3) In its capacity as the Smart Metering Entity, the IESO has had an important view to the development of the province's smart metering system over the past five years. The IESO notes that interactions between the existing smart metering system and the emerging class of third party service providers using Smart Grid technologies is forcing an important discussion about the nature of those interactions. These issues are addressed in both the OEB staff discussion paper and in several of the recommendations of the May 2011 report of the Smart Grid Forum, "*Modernizing Ontario's Electricity System: Next Steps."*

For the purpose of this submission, the IESO will confine itself to the first of these perspectives – the potential challenges and opportunities that Smart Grid technologies present. Further, these submissions focus on two of the Key Issue Areas in the staff discussion paper - cyber-security and interoperability.

**Challenges and Opportunities**

**Wholesale Markets and the Smart Grid: Value to Consumers and the Electricity System**

There is potential for the Smart Grid to enhance the operation of the bulk electricity system for Ontario and provide reciprocal benefit to consumers who will, as a matter of course, use Smart Grid-related products and services. In January of 2012, the IESO's consultations on the future development of the wholesale market ("the Market Forum") identified the link between customers, Smart Grid technologies and the opportunities afforded by a dynamic market price signal. The Market Forum's report states:

> *"The opportunity to engage the demand-side is, challenging as it is, worth pursuing. Consumers have been able to benefit from technological and service developments in*

*virtually every other product and service in our economy. These benefits should derive from electricity services as well. A customer-focussed electricity system would look to consumers as a key resource to help meet its capacity and operability needs."*[1]

*"The real opportunity for engaging the demand-side of the market is less through expecting customers to manually change their energy usage than through aggregation of customer demand and the use of Smart Grid and smart home technology. An enhanced price signal...can provide a triggering mechanism that will allow the Smart Grid to automatically adjust customer electricity usage."*[2]

Aggregation of customer demand using Smart Grid technologies and interactions with the wholesale market was also the focus of one of the recommendations of the Ontario Smart Grid Forum in its 2011 report:

*"The role that aggregators can play in delivering benefits to consumers via the Smart Grid should be investigated and, where appropriate, specific recommendations should be developed to facilitate their participation in the market. The Forum and its Corporate Partners Committee will work with industry to address this issue."*[3]

The integration of Smart Grids and wholesale markets is also the subject of broader industry research connecting markets to the Smart Grid. A recent KEMA Consulting report examined the role of wholesale markets in two case studies involving fast response energy storage for ancillary services and demand response. In its report, KEMA argued that, *"...wholesale markets are helping to foster innovation and grow markets in alternative technologies by providing:*

- *Opportunities to take risk in return for a chance at financial reward*
- *Transparency in valuation of services*
- *A level playing field for participants to sell services across a wide customer base*
- *A framework that determines winners based on price and performance."*[4]

**Next steps towards unlocking the value of Smart Grids in Ontario**

The IESO is taking the first steps in connecting empowered consumers, dynamic price signals and Smart Grid technologies. The IESO is participating in a joint project with North America's system/transmission operators via the ISO/RTO council (the "IRC") to adapt demand response interoperability standards for use by wholesale markets. This project is working with various standards development organizations such as the U.S. National Institute of Standards and Technology (NIST) and the North American Energy Standards Board to ensure that the resulting interoperability standards are openly available to public utilities and private industry. Recently, NIST announced a priority action plan[5] to ensure that the products from this effort find their way into their highly-influential interoperability Catalogue of Standards. The resulting products

1 IESO, "Market Forum Report", page 7.
2 Ibid. page 7.
3 Ontario Smart Grid Forum, "*Modernizing Ontario's Electrify System: Next Steps*.", Recommendation, page 7.
4 KEMA, "KEMA White *Paper: Innovation in Competitive Electricity Markets",* page 3.
5 Specifically, PAP19: Wholesale Demand Response (DR) Communication Protocol.

from this effort will allow for a more open and transparent means of aggregating demand response, electric vehicle charging, ancillary services, and other Smart Grid-related services. With NIST support, these standards will be widely used across North America. Ontario cannot be left behind. Ontario must remain in step with common standards to ensure that we can make use of the broadest possible array of Smart Grid-related products and services.

**Key Issue Area 5 -** ***"Which model is preferred: (a) privacy and cyber-security requirements as part of the approval of Smart Grid plans; (b) privacy and security as conditions of licence either by licence amendments or code requirements; or, (c) a combination of both? What guidance should the Board provide regarding evidence of co-ordination?"***

**Emerging Challenges and IESO Obligations**

The IESO and the OEB have responsibilities to ensure Ontario's adherence to North American-wide standards for security and reliability. Soon those standards will be affected by emerging issues from the Smart Grid and it will be essential that the IESO and OEB coordinate efforts to stay ahead of these developments.

The North American Electricity Reliability Corporation ("NERC") is one of many industry organizations that have been examining the potential security implications of the Smart Grid on the bulk electricity system. As observed in NERC's December 2012 report, "*Reliability Considerations from Integration of Smart Grid*":

> *"Historically, the static and dynamic character of distribution systems has been well understood and predictable. Smart Grid systems can change this character, the impacts of which need to be addressed to ensure continued reliable operation of the bulk power system. Further, with the adoption of Smart Grid innovations on the distribution system, additional cyber vulnerabilities may be introduced from either malicious attacks or human factors."*[6]

For the IESO and other system operators across North America, this is an issue of great importance. As noted in the NERC report[7], unlike many other industries, the electricity sector cannot simply shut down communication and "re-boot" when a cyber event occurs. The bulk power system must always be operated continuously and reliably – even during a cyber event.

[6] NERC, "*Reliability Considerations from Integration of Smart Grid*" page III.
[7] NERC, "*Reliability Considerations from Integration of Smart Grid*" page 70.

**Cyber Security and the Regulator**

Cyber-security issues in the electricity system go beyond the traditional boundaries of the regulated industry, fuelling the complexity and scope of the challenge for our sector. This is also noted in the NERC report where it is observed that, "*The strength of interoperability design of Smart Grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability, through a variety of entrance and exit points."* [8] The Report identifies basic steps to mitigate these risks, and later in the same report states, *"cyber security, physical security, compliance, business continuity planning, risk management and incident response are among many responsibilities of an enterprise security program; however, they need to be treated as a coherent unit, with objectives, controls and repeatable processes. With the addition of Smart Grid devices/systems, the importance of these activities multiplies."*[9]

NERC's concerns about Smart Grid-related cyber security issues should be front and centre in the OEB's deliberations over an appropriate framework for the Ontario electricity industry. Both the OEB and IESO play critical roles in ensuring that Ontario adheres to various NERC standards and remains in step with the rest of North America in that regard.

As NERC's Critical Infrastructure Protection standards continue to evolve to accommodate emerging issues, the OEB must ensure continuity and consistency with that practice. At present, U.S. authorities are working to ensure that emerging interoperability standards for the Smart Grid are thoroughly tested and screened from a cyber-security perspective – a point further discussed in the next section of this submission. Ontario must make use of that work in order to avoid confusion, duplication of effort and inefficient use of resources. The other significant challenge for the OEB in this area is to ensure that those standards apply to all those who will have an operational impact on the electricity system.

**Security and Third Party Service Providers**

Security issues arising from emerging Smart Grid-related activities of third party service providers will pose challenges to the industry, and more particularly, will pose challenges to the OEB. The questions posed in Key Issue Area # 5 address the appropriate means (either through Smart Grid approval plans or as part of licence requirements) for the OEB to review privacy and cyber-security issues. However, the IESO's main concern relates to how new products and services under the control of non-licensed entities may affect the overall security of the Ontario electricity system. The IESO recognizes that these concerns have to be balanced with the need to allow competition in the "smart homes" space to flourish – one of the key recommendations of the Ontario Smart Grid Forum in their May 2011 report, "*Modernizing Ontario's Electricity System: Next Steps."* The Board may also consider how effective cyber-security requirements will be if non-licensed parties are not subject to an equivalent, comprehensive security framework. Many of these new services may not meet the current definition of distributor or retailer activity, and yet may have the ability to affect the operation of the power grid. Can and

[8] Ibid. page III
[9] NERC, "*Reliability Considerations from Integration of Smart Grid*" pages 84.

should these new activities be licensed and regulated? Can the OEB create a security framework that includes new players? If not, then it may consider working in cooperation with various federal authorities to ensure that some level of equivalent safeguards are in place.

This is also where the IESO has a unique view to the cyber security implications of smart-grid related activities. As the operator of the bulk electricity system, the IESO must have a comprehensive security framework that encompasses all entities that might have a direct or aggregate/indirect impact on reliability and security – regardless of whether those entities meet the formal definition of a market participant, a distributor or a retailer. However, any measures taken will be limited in effectiveness if a gap in regulatory oversight allows various unregulated actors in the Smart Grid to become a weak link in the security of the electricity system.

The confusion over cyber-security roles has been indentified at the national level, as noted in a December, 2010 report by the Canadian Department of National Defence:

> *"Where there are multiple stakeholders, regulatory authorities and different levels of government, each required to engage collaboratively in the security and emergency management aspects of critical infrastructure and related mitigation and resilience issues, a clear and undisputed lead department with the necessary powers of direction and control will be crucial. Good governance further requires that there be shared principles and agreed mandates, clear terms of reference, coordination mechanisms and accountability protocols in place as part of the policy approval and resource acquisition road map. If these are lacking, there will be confusion about roles and responsibilities; how expressed "concerns" can be prioritized at all levels of government; and which individuals and organizations are to be held accountable for policy implementation."* [10]

The report concludes that the extensive delays in creating a national strategy for critical infrastructure protection can be traced back to the lack of clarity on roles and responsibilities of the different levels of government.

Cyber-security is emerging as a critical issue for the Smart Grid, and extends well beyond the traditional boundaries that the OEB and other regulators have operated in. A comprehensive response from the OEB should recognize the practical limits of its authority, clearly articulate those limits to the industry, and proactively work with other institutions to address the potentially serious gaps in cyber-security that cannot easily be addressed solely by codes and licence conditions.

The OEB must be mindful that it is developing a cyber-security framework for the Smart Grid in an environment where regulatory authority and policy is still evolving. The Department of Public Safety's 2010 document, "*Canada's Cyber Security Strategy*" stated that, *"strengthened public/private partnerships will be fostered through existing structures and organizations, such*

[10] Canadian Department of National Defence, Centre for Operational Research & Analysis, Angela Gendron "Critical Energy Infrastructure Protection in Canada", DRDC CORA CR 2010-274, December, 2010, page 27.

*as critical infrastructure sector networks. Cross sector mechanisms will also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security."* [11] However, it remains to be seen what the precise nature of those "public/private partnerships" will be or whether their scope will be adequate to address the unregulated companies falling outside of such a framework.

The cyber-security framework for Ontario, and particularly, in the field of emerging Smart Grid service providers is currently lacking in several areas including regulatory authority, identification and enforcement of standards, and information sharing. The OEB may not be able to address all of the issues in this area, but it needs to clearly identify which aspects of the cyber-security framework it seeks to enforce, and where there may be gaps that have to be dealt with in partnership with other institutions. The IESO encourages the OEB to consider Ontario's cyber-security framework through the lens of inter-agency cooperation to ensure that gaps in regulatory authority do not undermine the security requirements the OEB imposes on Ontario's regulated entities.

**Key Issue Area 8 – "*How should the Board take cognizance of international standards processes?"***

Ontario's success with Smart Grid deployment will depend on its ability to remain in-step with broader interoperability standards currently being developed. Similar to cyber-security issues, the OEB must strike a balance between over-regulation in critical areas, and supporting Ontario's electricity industry in a manner that encourages the use of widely-accepted interoperability standards. The goal should be to ensure that Ontario's energy sector has the widest possible choice of technologies and tools to draw from, that it benefits from competition, and is able to adapt to a changing technological landscape. In this regard, there are lessons from recent regulatory experiences in other jurisdictions.

The IESO applauds the OEB for its participation in emerging Smart Grid-related interoperability standards discussions. The OEB is participating alongside the IESO and other Ontario electricity sector organizations in the Smart Grid Task Force of the Canadian National Committee of International Electrotechnical Commission ("CNC/IEC"), which is in the final stages of a national report. This report will likely have recommendations for provincial regulators and will be of great interest to the OEB.

In 2011, the U.S. Federal Energy Regulatory Commission ("FERC") considered whether to codify five standards proposed by the National Institute of Standards and Technology (NIST)[12] and reviewed the general implications of Smart Grid Interoperability Standards, by asking, among other things:

- Should standards indeed be "enforceable" by a regulator?

[11] Government of Canada "Canada's Cyber-security Strategy" ISBN: 978-1-100-16934-7, page 12.

[12] U.S. Federal Energy Regulatory Commission, Docket No. RM11-2-000, "*Smart Grid Interoperability Standards"* (Issued July 19, 2011) Specifically: IEC 61968: Application Integration at Electric Utilities-System Interfaces for Distribution Management; IEC 61970: Energy management system application program interface; IEC 61850: Communication Networks and Systems for Power Utility Automation; IEC 60870-6 series: Telecontrol protocols compatible with ISO standards and ITU-T recommendations; and IEC 62351: Power systems management and associated information exchange – Data and communications security.

- What constitutes "sufficient" industry consensus to use a standard in the first place?
- What aspects of interoperability should a regulator concern itself with exactly?
- How should a regulator approach "normative references" to a standard whose content is in fact governed by an international body well outside of its jurisdiction?
- Does a regulator need to concern itself with the degree to which a standard addresses cyber-security issues, or rely on the work of the standards body that developed it?

In its decision FERC stated that it was satisfied with the "comprehensiveness" of NIST's stakeholder process, and determined that the kind of stakeholder engagement efforts run by NIST would ensure thoroughness from a security assessment standpoint and that the body of recognized standards are continuously improved. FERC stated, "*These planned improvements include an enhanced* Smart Grid Interoperability Panel (*SGIP) role in reviewing existing as well as new Smart Grid interoperability standards, the establishment of a preliminary testing process, the establishment of a process to identify cyber security design principles, and efforts to better address reliability and implementation concerns within the SGIP process. Therefore, we encourage utilities, Smart Grid product manufacturers, regulators, and other Smart Grid stakeholders to actively participate in the NIST interoperability framework process to work on the development of interoperability standards and to refer to that process for guidance on Smart Grid standards.*"[13]

These considerations will also need to be addressed within Ontario's interoperability framework. Proper testing and security assessment of standards will be required. The standards will also need to be clear and accessible, however they cannot be an artificial barrier to legitimate competition and the development of Ontario's Smart Grid. While not all of these responsibilities belong with the regulator, the OEB may help regulated entities turn to the appropriate body of interoperability standards to use. The upcoming report of the CNC/IEC will likely identify options in this regard and we encourage the OEB to consider the recommendations coming out of this report.

The IESO also encourages the OEB and the electricity industry to consider the work of NIST and its Smart Grid Interoperability Panel ("SGIP"). The SGIP maintains a catalogue of standards that have undergone development by the sponsoring standards bodies, review by dedicated stakeholder groups, rigorous testing, and a cyber security and architecture review. Once these reviews are complete, the standards are then added to SGIP's Catalogue of Standards. At present, over 160 different standards are at various stages of the SGIP review process.[14] Once all of these standards have been added to the Catalogue, they will have a significant influence over the development of technologies in every aspect of the Smart Grid, from distribution automation equipment, to how smart appliances will communicate within a customer's home. Participation in the SGIP processes could offer the OEB and other Ontario electricity sector

[13] U.S. Federal Energy Regulatory Commission, Docket No. RM11-2-000, "*Smart Grid Interoperability Standards"* (Issued July 19, 2011), page 7.
[14] U.S National Institute of Standards and Technology, Smart Grid Interoperability Panel website, "CoS Standards Review Pending".

organizations not just a means of staying abreast of developments in these areas, but allow Ontario to provide input on the development of these standards.

**Next Steps**

The Smart Grid is more than just a technological phenomenon – it is changing the electricity sector, and the potential benefits of these developments extend far beyond our sector. As recently noted in a report by the Waterloo Global Science Initiative, *"Infrastructure such as Smart Grids – allowing information and communication technology to be interwoven with the electrical grid systems, along with other enabling elements – are emerging. Together they produce a net energy system that is flexible, responsive and efficient, compatible with electric transportation and a bi-directional flow of electricity."*[15]

Not only will customers be able to buy, sell and store power in a sophisticated manner, this new flexibility will generate new opportunities and activities beyond those which are currently licensed and regulated by the Ontario Energy Board. These new activities can be supported by Ontario's wholesale electricity market for the benefit of customers and the reliable operation of the bulk electricity system, and the IESO is already taking early investigatory steps in that regard.

The OEB will need to take action in the context of what is being done at a national and international level. To act in isolation will put Ontario's Smart Grid at risk for both commercial isolation and cyber security vulnerabilities. While many of the new actors in the Smart Grid may have an impact on these issues, they may not fall within the regulatory authority of the OEB, but may nonetheless present a challenge to the objectives the OEB is seeking to achieve. The OEB may need to consider how it can address these gaps to protect Ontario electricity consumers. Much can be gained through cooperative work with other agencies and the IESO looks forward to assisting these efforts wherever possible.

Brian Rivard
Manager, Regulatory Affairs
Independent Electricity System Operator

[15] University of Waterloo, Jatin Nathwani, Jason Blackstock et. al., Waterloo Global Science Initiative, "*Equinox energy 2030 Blueprint A technological roadmap for a low-carbon, electrified future*". Page 41.