Remarks of the IESO Regarding:

Panel 2: Scope and Implementation of a New or Modified Standard

Douglas Thomas, Vice-President and CIO
Independent Electricty System Operator

FERC Technical Conference on
Supply Chain Risk Management (Docket No. RM15-14-000)

January 28, 2016

ieso
Connecting Today.
Powering Tomorrow.

Contents

Introduction

First of all, I would like to express my appreciation for the Commission allowing me to present and discuss today, the seven topics that are under consideration by this panel. As the last presenter for this panel I recognize that my colleagues have already addressed these topics in some detail so I will endeavor not to be unduly repetitive in my remarks and rather, will, as the only representative from Canada, focus on Canadian, and more specifically Ontario, aspects that I respectfully suggest should be considered. Finally, I would note that the Canadian and Ontario considerations pertain to all three panels and I would therefore appreciate your patience as some of my comments touch on topics that are being considered by the other two panels.

First I would like to provide you with a very brief background on the IESO, the nature of our business, and the unique aspects of how we fit into the NERC regulatory framework. I will then discuss the seven topics requested by this Technical Panel from an IESO perspective before finally taking a few moments to discuss the seven topics from a wider Canadian and Ontario viewpoint.

The Ontario Independent Electricity System Operator (IESO)

The IESO is an independent electricity market operator and reliability coordinator for the province of Ontario. Our business is very similar in nature and function to the independent system operators in the United States with which you are obviously very familiar. The IESO is a not-for-profit, non-share, corporation owned by the Province of Ontario, and our Board of Directors is appointed by the Ontario Government through the Minister of Energy. We are a member of the ISO/RTO Council (IRC) but our remarks here today do not represent the IRC's positions. The IESO is also a member of the Canadian Electricity Association (CEA) but, once again, our remarks do not represent the CEA's positions.

The IESO is subject to the NERC Reliability Standards through various memorandums of understanding between the IESO, NERC, the Ontario Energy Board and NPCC. I will further explain these entities and relationships when I address the Canadian and Ontario aspects for consideration. The IESO is the only organization in Ontario that is directly subject to the NERC Reliability Standards through the memorandums and is audited by NPCC. All other BES asset owners in Ontario are subject to the NERC Standards through the IESO as mandated by our Market Rules. Enforcement of the standards in Ontario is the responsibility of the Market Assessment and Compliance

Division of the IESO (commonly referred to as MACD) which is a "ring fenced" organizational unit within the IESO. MACD manages compliance enforcement for Ontario in cooperation with NPCC.

Panel Two Discussion Topics

IDENTIFY TYPES OF ASSETS THAT COULD BE BETTER PROTECTED WITH A NEW OR MODIFIED STANDARD.

I will now turn my remarks towards the seven topics under consideration by this panel.

I believe, as do many of my colleagues that determining the appropriate applicability scope for any standard of this nature is paramount to its success and enforceability. The NERC standards are focused on the reliable operation of the bulk electric grid in North America. As such, any new standard or requirement must be focused on the same objective. The NERC CIP standards are very explicit in the determination of applicability of the standards to assets, specifically that the assets are essential to the reliable operation of the grid. Any new standard or requirement must apply to the same assets as those identified through the current CIP standards.

The CIP standards are focused on all cyber security aspects of applicable assets. Any new standard or requirement related to supply chain cyber security risk must also focus on those same aspects of hardware, software as well as people and services, irrespective of whether it is network, infrastructure, or solution based.

I feel that it is important to specifically address the services aspect of supply chain management. In today's environment an ever increasing reliance on cloud based services is broadening the horizon for security risks. While a cloud service may not be considered an asset per say, a cloud service represents very similar risks from a supply chain perspective and any standards should include cloud based services in the same manner as physical assets.

IDENTIFY SUPPLY CHAIN PROCESSES THAT COULD BE BETTER PROTECTED BY A STANDARD

I submit that there are three categories of processes that need to be considered in an independent but interconnected way. These three categories of processes are: procurement, design/build/implement, and contract management.

Procurement processes are those processes that organizations use to procure goods and services. Supply chain risks are evident through all aspects of the procurement

processes both internal and external to the organization. Standards are needed to ensure security concerns are addressed during the procurement processes to ensure that the security needs of the asset owner are clear to the vendor or vendors which will ultimately be ensconced within a procurement contract.

Design/build/implement processes typically engage multiple parties such as product vendors, service vendors, integrators and consultants. These processes also engage internal asset owners and business functions such as IT, Operations (specifically engineering) and Human Resources. Standards are required here to ensure that vendor products are designed to incorporate security from a number of perspectives (e.g. built in a secure environment with secure related best practices such as secure coding and implementation in a secure manner). As the standards can only be enforced with the asset owner, meeting the standards must be done through procurement contracts, so the standards need to focus on the necessary contract requirements to meet the risk mitigation needs associated with the design/build/implement processes.

Strong and robust contract management processes are keys to successful supply chain risk management as they are the only means available to an asset owner to enforce security requirements. Standards are needed to address contract requirements not only for the original purchase and delivery, but also for the ongoing maintenance including delivery of enhancements, patches, and other services. Standards are also needed to address the establishment and termination of the contracts themselves.

IDENTIFY CONTROLS OR MODIFICATIONS THAT COULD BE INCLUDED IN THE STANDARD.

Controls should be risk based and consistent with existing CIP standards, following the traditional security model of confidentiality, integrity and availability. Controls should be addressed through the standards to meet the needs of each of the three process areas I discussed previously (i.e. procurement, design/build/implement, and contract management).

Within the procurement process, controls addressing confidentiality and integrity should be identified, including controls to ensure procurement mechanisms such as Requests for Information (RFIs), Requests for Proposal (RFPs) and Request for Quote (RFQs) do not expose sensitive information beyond those who need to know. This can typically be achieved through non-disclosure agreements with qualified bidders. Criteria to establish qualified bidders could be required and standardized. Security language for procurement instruments could also be standardized.

Within the design/build/implement processes, controls need to be required of the vendor or service provider through appropriate language in both the procurement contract and if appropriate, the subsequent “Statement of Work”. Guidance with

respect to contract language for the controls can be obtained from the Department of Energy (DOE) document "Cybersecurity Procurement Language for Energy Delivery Systems" which provides extensive examples of procurement language. I would also suggest that the standards require controls within the documentation of the design, build and implementation processes to ensure that security is considered in any activities that the asset owner itself undertakes. These controls could include requirements to ensure that secure practices are included in process documentation and observed during internal activities in the associated processes.

Contract management processes are essential to the ongoing care and feeding of the supply chain. It is important to ensure sufficient controls are in place to make sure contracted parties continue to address security risks as they are laid out in the contract. Standards should address the need to periodically review contract performance. For example, where contracts stipulate the need for a third party security audit or assessment of the vendor's security controls, the standard should require the entity to review subsequent audit results or assessments throughout the lifetime of the contract. I recommend that the standard drafting team consider including requirements to cover contract management related risk and control issues.

IDENTIFY EXISTING MANDATORY OR VOLUNTARY STANDARDS OR SECURITY GUIDELINES THAT COULD FORM THE BASIS OF THE STANDARD.

There are several well-known guidelines and standards available such as NIST 800-53, NAESB and ISO 27001. One guideline that may not be so well known but is very relevant, is the "Cybersecurity Procurement Language for Energy Delivery Systems" developed and published under the auspices of the US DOE.

Two other very relevant standards are:

- ISO/IEC 27036: Information Security for Supplier Relationships (Four Parts).
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

ADDRESS HOW THE VERIFICATION OF SUPPLY CHAIN RISK MITIGATION COULD BE MEASURED, BENCHMARKED AND/OR AUDITED.

I submit that verifying supply chain risk mitigation by the entity that is subject to the standard is relatively straight forward and can be addressed through existing NERC compliance auditing practices for the CIP standards. The obvious challenge is how to verify third parties risk mitigation practices. To address this challenge I propose that

standards require the entity to obtain third party assurance through SSAE 16 type II audits performed by reputable third party audit firms. To ensure that the SSAE 16 audit meets the needs of the entities supply chain risk mitigation the standards will need to define the necessary control objectives to be included in the audit. These control objectives would, in turn, need to be ensconced in any procurement or service contract.

PRESENT AND JUSTIFY A REASONABLE TIMEFRAME FOR DEVELOPMENT AND IMPLEMENTATION OF A STANDARD

Development of a standard of this nature is complex and will require extensive stakeholdering with many divergent entities including both those that are directly impacted such as the applicable BES entities, as well as those that are indirectly impacted such as product vendors and service suppliers. Taking this into consideration along with experience in developing the CIP version 3 and version 5 standards the process could take three to four years. However as this is an existing and potentially significant risk I suggest that every effort be made to have the standards in place and enforceable within two years of the FERC order.

DISCUSS WHETHER A STANDARD COULD BE A CATALYST FOR TECHNICAL INNOVATION AND MARKET COMPETITION.

I believe that this initiative will, out of necessity, drive innovation and competition. If our industry establishes security practices and requirements that are consistent across the industry, vendors and service providers will have concrete requirements they can use to address cyber-security risks. As all vendors and suppliers will be working towards the same requirements they will be able to design and implement competitive cost effective controls and compete on a level playing field. Additionally, as vendors and service providers implement controls they will be able to leverage those controls to compete not only in the oil, gas, and water industries, but also potentially within manufacturing, transportation and other industries that rely on control systems. I believe that our industry is poised to be a major catalyst for innovation and competition through these standards, which will have benefits well beyond our industry but in a way that does not go beyond what our needs are within the electricity industry.

Canadian and Ontario Aspects for Consideration

POLITICAL JURISDICTION

It is important to understand the national and provincial jurisdictions with regards to electricity in Canada and Ontario. Significantly, most of the relevant regulatory framework is provincial based. At the national level, The National Energy Board (NEB)

exercises federal jurisdiction over electricity exports and over international and interprovincial power lines. Natural Resources Canada (NRCan) works with other government departments, the provinces and territories, and other Canadian and international partners to address current and future energy needs while considering new policies, practices, and technologies. NRCan does not have regulatory responsibility over electricity in Canada.

As I have mentioned, most of the electricity regulatory framework is within provincial jurisdiction. As the IESO operates in Ontario I will speak to the Ontario framework. In Ontario the *Electricity Act, 1998, S.O., 1998 Chapter 15* (as amended) established the Independent Electricity System Operator (IESO). The IESO reports to the Ontario Legislative Assembly through the Minister of Energy and is licensed and regulated by the Ontario Energy Board. The IESO is responsible for ensuring an adequate, long-term supply of electricity for Ontario, as well as operating the electricity market and directing the operation of the bulk electrical system in Ontario. More specific responsibilities within that broad mandate include ensuring the reliability of the BES in Ontario, and performing short and long term planning in addition to managing conservation efforts and generation procurement contracts.

The Ontario Energy Board (OEB) is the regulator of the province's electricity and natural gas sectors. The OEB is established through the *Ontario Energy Board Act, 1998*.

APPLICABILITY OF NERC STANDARDS IN CANADIAN PROVINCES

The NERC Reliability Standards are applied differently in each of the provinces that have established agreements with NERC. In Ontario, the IESO administers and enforces the Reliability Standards. The OEB, as the regulator, is a quasi-judicial tribunal that establishes licensing provisions and enforces those licensing provisions through hearings and rulings. In Ontario there is no body that formally approves NERC Standards. By default, NERC Reliability Standards become enforceable in Ontario coincidental with FERC approval in the US., however there is provision for an Ontario entity to apply, within 21 days of the IESO posting a new or amended reliability standard on its website, to the OEB for a review of a particular standard or requirement. If the OEB conducts a review it has the authority to to stop the standard from applying in Ontario and to refer it back to the standards authority.

CANADIAN CONTRACT LAW

Canadian contract and tort law is similar in nature to the US with the possible exception of jurisdiction. Typically jurisdiction is specified within the contract as a single jurisdiction within a Canadian contract. Therefore contracts that are established in Ontario will specify Ontario as the jurisdiction for enforceability purposes.

Import and export restrictions should also be considered with respect to supply chain security. For the most part, the North American Free Trade Agreement (NAFTA) greatly simplifies such restrictions, but certain security related restrictions may still apply. For example the US has restrictions on certain products that use encryption methodologies considered sensitive to the US. These restrictions may not impact supply chain standards but should be considered to ensure Canadian entities are not precluded from complying with certain encryption standards or other security related restrictions.

Other legal considerations that should be considered are copyright law, trademarks, competition, etc. Canadian case law in this area is still evolving and it is not likely to present any barriers to supply chain standards but it should be considered when developing the standards.

CANADIAN REGULATIONS AND STANDARDS

At present there are no specific regulations or standards that pertain directly to supply chain cyber security issues. NEB standards that pertain to international or inter-provincial transmission lines allow for the NEB to include and I quote, "requirements relating to the mitigation of any adverse effects that the operation of the facilities may have on the reliability of any power systems to which the facilities are interconnected" within a license or permit to construct or operate a transmission line. There is a potential that the NEB could include supply chain security controls within a license or permit, however to the best of my knowledge, there are no such cases to date.

The smart grid arena is rapidly evolving in Canada and there is a recognized need for security standards for smart meters. There is also a concern around privacy that is not unique to Canada but does have Canadian specific nuances, such as out of country personal information storage and access. While it is not my intention to go into detail today, I suggest that it will be important to ensure privacy issues are considered in the development of any standards.

Closing Remarks

In closing, I would like to reiterate that the IESO supports and encourages the commission in proceeding with an order to develop and implement one or more standards to address the significant security risks inherent within the supply chain of control systems and products that are used to maintain the reliable operation of the BES. We feel that leveraging the existing CIP version 5 standards to determine scope is an appropriate means to make sure we remain focused on maintaining reliability.

And finally, as a Canadian entity, the IESO respectfully suggests that NERC is the only governing body that has international agreements in place to govern and enforce compliance with standards and requirements. As the supply chain is essentially the same for all North American entities, the IESO recommends that FERC take into consideration international aspects when determining the most effective approach to addressing supply chain security risks.

Thank you for allowing me the opportunity to address this technical panel. I look forward to continued engagement on this very important issue of cyber-security supply chain risk.