Written Statement of Francis Bradley
Chief Operating Officer & Vice President, Policy Development
Canadian Electricity Association
U.S. Federal Energy Regulatory Commission Docket No. AD16-15-000
Reliability Technical Conference
Panel III: Grid Security
June 1, 2016

Introduction

Good afternoon Chairman Bay and Commissioners.

My name is Francis Bradley and I serve as Chief Operating Officer and Vice President, Policy Development of the Canadian Electricity Association (CEA). CEA is the national, authoritative voice of the Canadian electric utility industry.

Along with our U.S. counterparts, Canadian stakeholders share a common vision and stake in the success of the international NERC regime. CEA therefore remains very grateful for the opportunity to participate in this annual conference.

In that regard, I am particularly appreciative of the chance to participate on this panel. Not only do CEA members have equal skin in the game when it comes to security of the North American grid, but the nature of security threats and vulnerabilities themselves demands coordinated partnership and action – not solutions pursued in isolation.

In this spirit, my remarks today will focus on the following themes: (1) NERC standards and their optimal role going forward; (2) the increasing importance of effective partnerships between industry and government; and (3) the imperative of applying a North American lens to the pursuit of grid security solutions.

1. NERC Standards

Regarding NERC's cyber standards, they now need time to mature and demonstrate their effectiveness.

Recent years have witnessed significant churn in the modification of CIP standards. Like our U.S. peers, CEA members have invested unprecedented time and resources in preparing for Version 5 compliance. CEA strongly believes that these standards must

be given the chance to mature, with industry granted sufficient opportunity to cultivate experience in implementation.

A major benefit of granting Version 5 adequate time for maturation is enabling positive unintended consequences to come to fruition. A few CEA members, for example, report that early experience in preparing for V5 implementation has improved their ability to detect and mitigate human error.

NERC CIP standards will continue to serve as a critical foundation upon which we base the protection of electric grid assets and systems. CIP standards can only protect us from the threats and hazards of the past, and we must continue to look to the horizon to identify new risks. We rely upon our strong partnerships with government for assistance because we understand that standards are not the optimal solution to increasingly-sophisticated and rapidly-evolving threats and vulnerabilities.

2. Industry-Government Partnerships

There are many examples of industry-government partnerships, and they are proving to be capable of addressing security challenges in ways which are set apart from, but complementary to, NERC standards.

The Electricity Subsector Coordinating Council or ESCC is an obvious example. One illustration of the increasing effectiveness of this CEO-level body is the number and nature of initiatives launched since FERC's last reliability conference. In the ensuing months, the ESCC has organized new work streams focused on mutual assistance for cyber incidents; support for new research on electromagnetic pulse threats; supply chain management; and enhanced background investigations for utility personnel.

The ESCC is also playing a critical role on another top priority in the grid security arena – information sharing. With ESCC support, new information sharing technologies like CRISP are being refined, while the capability of NERC's E-ISAC is being bolstered.

The ESCC's engagement with government continues to yield dividends for enhanced security. The forum is uniquely-suited to injecting momentum into its initiatives and doing its work with the nimbleness required to tackle moving target challenges.

Finally, one example of a new industry-government partnership in Canada which reinforces the value of these collaborations is the Canadian Cyber Threat Exchange, or CCTX. Launched in early 2016 by some of the largest firms in Canada, CCTX is a new hub for automated sharing of cyber threat information between the private and public

sectors. CCTX is attracting significant interest from firms of all sizes, and is further underscoring how robust, creative partnerships between industry and government are increasingly becoming the key tools in enhancing the grid's overall security posture.

3. Grid Security in a North American Context

The third and final theme which I would l like to explore is the imperative of sustaining a coordinated approach across North American on grid security solutions.

For its part, CEA is committed to contributing to the success of vital forums like NERC and the ESCC. What's more, we remain confident that security outcomes are optimized when there is built-in recognition of the need for and value in ensuring applicability of solutions across the North American landscape. The number of milestones achieved on these fronts continues to grow – a few of which I will highlight briefly:

- Canadian stakeholders remain engaged in numerous ESCC work streams which have direct cross-border relevance:

    - Expansion of the traditional mutual assistance model (which has always had a significant cross-border component) into the cyber domain;
    - Efforts to position the E-ISAC as the center of gravity for electricity sector information sharing in North America; and
    - Transformer transportation contingency planning, with CEA facilitating engagement with Canadian-based railways operating in the United States.

- Major incident response exercises are now beginning to appropriately simulate the likelihood of cross-border impacts of coordinated attacks and natural disasters (e.g. NERC's GridEx III scenario included widespread outages and events in Canada, while a recent ESCC scenario simulated earthquake-induced damage in Canadian and U.S. regions of the Pacific Northwest).

- The U.S. *FAST Act* requires: (i) the U.S. Department of Energy (DOE) to consult with Canadian and Mexican authorities prior to issuing new grid security emergency authority; and (ii) DOE and FERC to develop voluntary information sharing protocols with Canadian entities. CEA hopes that the latter provision is implemented so as to bolster the E-ISAC's unique role in North America.

- On the margins of a historic state visit in March 2016, President Obama and Prime Minister Trudeau pledged further cooperation on clean energy. Their plan includes a deliverable on a joint strategy for strengthening the security and

resilience of the North American grid. This strategy will be released by end of 2016, and will address many of the topics flagged for this panel.

These and other actions bode well for cementing grid security as a cooperative, North American enterprise going forward. However, sustained vigilance is required to ensure that a continental lens is continually applied to these challenges and that solutions are more effective as a result.

Conclusion

Once again, I thank the Commission for the privilege of being here today and would be happy to answer any questions that you may have.