



Protecting the Integrated North American Grid – A Canadian Perspective

Reliable, Secure Power is the Canadian Electric Utility Industry's Top Priority

Providing a reliable, secure and affordable electricity supply is the top priority for electric utilities in Canada.

Members of the Canadian Electricity Association (CEA) recognize that reliability and security are the fundamental benchmarks used to assess our performance in meeting the needs of our customers in Canada and the U.S. In 2002, the province of Ontario became the first jurisdiction in North America to make reliability standards mandatory and enforceable. Since then, each of the provinces comprising the Canadian portion of the North American bulk power system has established a framework for the adoption and enforcement of standards. The Canadian electric utility industry continues to be a leader in improving its operational performance and enhancing its proactive, collaborative approach to ensuring system reliability and security.

The U.S.-Canada Electricity Relationship

The Canadian and U.S. electric transmission systems are physically interconnected at over 30 points, forming a highly integrated North American grid. This international bulk power system allows for cross-border trading in electricity, assuring – amongst other things – a higher level of reliability for consumers, efficiencies in fuel management, efficiencies in system operation, and greater access to low-emitting and competitively-priced electricity resources. Each year, Canada exports between six and 10% of its overall production to U.S. markets. Canadian utilities are therefore critical to the reliability of the North American transmission network and to overall U.S. energy security.

Shared Grid Security Threats Require a Coordinated and Cooperative Response

Given the integrated nature of the grid, reliability and security cannot be achieved in isolation. Protecting the grid requires a coordinated approach between industry participants and governmental authorities on both sides of the border. In view of the challenges posed by increasingly sophisticated and malicious threats – including those emanating from cyberspace – such cooperation is an even greater imperative.

Recommendations for Enabling an Effective Coordinated Approach to Grid Security

CEA members are committed to working with all relevant stakeholders in exploring the best approaches for enhancing the security of our shared electric system. In step with this commitment, CEA continues to engage industry partners and governmental authorities in the U.S. With the aim of supporting ongoing efforts to craft appropriate solutions for securing critical electric infrastructure, CEA respectfully offers the following recommendations to help ensure that these solutions will be workable and effective in a cross-border context:

1. Support and enhance the existing processes at NERC to develop cyber and other security standards for the North American transmission grid.

The North American Electric Reliability Corporation (NERC) develops robust reliability and cyber security standards for users, owners and operators of the continent-wide grid. The NERC standards development process is driven by industry stakeholders in both Canada and the U.S.,

with technical expertise in grid security and other areas. The NERC process is particularly appropriate for the international grid, since it is based on the co-operative development of standards, takes into account the interests of diverse stakeholders and is respectful of jurisdictional sovereignty. Achieving the highest possible level of grid security will require continued collaboration between NERC, industry and governmental authorities in the ongoing development and improvement of strong cyber and other security standards.

2. *Ensure that any authority given to U.S. governmental authorities to address emergency situations is limited in duration and is coordinated with Canadian governmental authorities*

CEA members recognize that, as threats to the grid evolve and become more sophisticated, it may be necessary for governments to direct certain emergency action in the event of an imminent threat. CEA understands this need and believes that such authority must be limited only to specific, credible and imminent cyber or other security threats, be limited in duration, and be coordinated with Canadian governmental authorities.

3. *Require consultation, coordination, and information sharing between the appropriate U.S. and Canadian governmental authorities*

In situations where there is justifiable concern that events in one country can impact the security of electricity supply in the other country, mitigating actions need to be coordinated between those countries to ensure that the appropriate governmental authorities and entities are involved.

Canadian utilities presently engage in proactive information sharing with provincial and federal governments regarding cyber and other security challenges. Expedited information sharing between the U.S. and Canadian governments is equally critical to ensure that the necessary information is received by the entity in the best position to address a security situation.

To this end, CEA supports language (included in previously proposed U.S. legislation) which would outline the need to develop protocols for the bidirectional sharing of protected threat information between appropriate governmental authorities in Canada and the U.S.

4. *Address cyber and other security threats in a comprehensive manner across all industry sectors, with a focus on securing the most critical assets from the most urgent challenges*

Cyber and other security challenges affect all economic sectors, not just electricity. CEA believes that a framework for addressing critical infrastructure security should encompass all sectors. A sector-specific approach only covers one piece of a much larger initiative and could overlook crucial elements that are needed to address security threats in a comprehensive manner.

The public and private sectors must also work together to identify and satisfy the most pressing needs for securing critical infrastructure through prioritizing the issues and focusing limited resources. Establishing a clear understanding of the roles, responsibilities and tradeoffs involved in addressing security challenges is vital to such efforts. This is particularly relevant to those challenges associated with low-frequency but severe-impact events – such as the threat of a direct attack on critical infrastructure – for which planning, deterrence and response measures have traditionally fallen under government purview.

Continued collaboration between industry and government – both in and between Canada and the U.S. – will be essential to improving our collective understanding of the evolving threats to critical infrastructure and to strengthening our ability to address them effectively.

