



Canadian Electricity Association
Association canadienne de l'électricité

www.canelect.ca

STATEMENT FOR THE RECORD OF
THE CANADIAN ELECTRICITY ASSOCIATION
BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON ENERGY AND AIR QUALITY
HEARING ON
“PROTECTING THE ELECTRIC GRID FROM CYBER-SECURITY THREATS”

September 11, 2008

The Canadian Electricity Association (CEA), the national forum and voice of the evolving electricity business in Canada, is pleased to provide the following statement regarding U.S. legislation to protect the electric grid from cybersecurity threats. CEA's members account for the majority of Canada's installed generating capacity and high voltage transmission. In this statement, CEA provides comments on the House discussion draft. This statement also explains the importance of taking actions that are mindful of the interconnected nature of the North American transmission grid and the impact such actions could have on the reliability of the grid and on cross-border trade.

Background

The electric transmission systems of U.S. and Canadian utilities are interconnected with one another at numerous points, forming a highly integrated North American transmission grid. This integration allows for cross-border trading, which facilitates, amongst other things, a higher level of reliability for consumers, efficiencies in fuel and resource management, and efficiencies in system operation. These benefits, and the activities of companies investing and participating in markets on both sides of the border, serve citizens of the United States and Canada extremely well.

CEA

350 Sparks Street, suite 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - fax: (613) 230-9326 - info@canelect.ca

The voice of Canadian Electricity

350 rue Sparks, bureau 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - Téléc.: (613) 230-9326 - info@canelect.ca

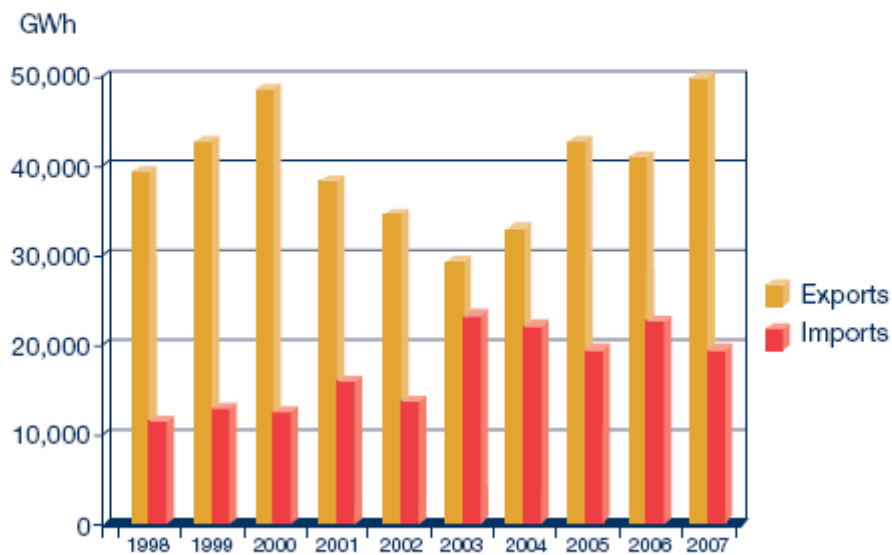
ACE

La voix de l'électricité canadienne



To provide perspective on the importance of the U.S./Canadian trading relationship, the chart below shows both exports from Canada to the U.S. and imports into Canada from the U.S. between 1998 and 2007:

Electricity Exports from Canada and Imports from the U.S., 1998-2007



Source: NEB Electricity Exports and Imports, Monthly Statistics, various years.

Canada is a net exporter of electricity to the U.S. The quantity of electricity exported from Canada to the U.S. has typically been 6 to 10 percent of Canadian production. At the same time, as the chart above demonstrates, electricity imports to Canada from the U.S. have increased over time. The North American market is borderless, and supply meets demand north to south or south to north as the market requires, to the advantage of consumers across the continent. Such electricity trade enhances the reliability of each country's electricity supply through the sale of surplus power, and mitigates risk by providing for power during times of emergency outages or periods of high electricity demand. Canadian utilities are therefore part of and therefore critical to the energy security of the United States, and the reliability of the North American transmission grid.



Addressing Cybersecurity Threats

The blackout of August, 2003 demonstrated the importance of carefully managing an interconnected grid for both the U.S. and Canada. In a matter of seconds, an estimated 50 million people in the Midwest and Northeast United States, and in Ontario, Canada experienced an electric power blackout. While the 2003 blackout was caused, in part, by a failure of a utility to comply with operating standards, the grid could be equally compromised following an exploitation of a cybersecurity vulnerability. CEA members are therefore sensitive to the potential for disruptions in electric service due to a system event anywhere on the international grid, including threats to cybersecurity.

CEA believes that any actions to address cybersecurity issues must be accomplished in a manner that recognizes the mutual inter-dependency of the interconnected Canada-U.S. transmission systems, and does not unintentionally imperil or downgrade reliability and erect barriers to cross-border trade. CEA believes that the best venue to address cybersecurity matters is the North American Electric Reliability Corporation (“NERC”). Through the reliability standard-setting model included in section 215 of the Federal Power Act, the NERC reliability standard-setting process allows for a balance of interests that ensures access to expertise from industry across the continent for the development of standards with continental application that can be approved by authorities on both sides of the border – be it FERC in the U.S., or any of the jurisdictional authorities in the Canadian provinces. This model recognizes jurisdictional sovereignty through the existence of remand provisions in the various pieces of Canadian and U.S. legislation underpinning the model and which is incorporated into the existing NERC standard setting procedures. This component assures that no governmental authority has the ability to unilaterally modify standards that would apply to the whole system, and that any



Canadian Electricity Association
Association canadienne de l'électricité

www.canelect.ca

variances are accommodated through the collective process. At the same time, it gives public authorities the confidence that the system has a government backstop, providing governmental authorities on both sides of the border with the confidence that standards developed through that process reflect their concerns.

CEA does recognize, however, that situations can arise that require emergency actions to be taken immediately to protect the reliability of the bulk power system. To the extent the NERC processes are unable to respond to such an emergency situation, CEA agrees that governmental bodies should be able to respond expeditiously to ensure that the grid is protected. In terms of U.S. governmental authority to respond to imminent cybersecurity threats, CEA has been working with key industry associations to provide input to legislative language that would provide FERC with authority to respond. The language would further allow FERC to establish interim measures with respect to threats identified in the Aurora advisory. CEA understands the need for authority to address emergency situations, although we believe that such authority must be limited only to cybersecurity emergencies and must be of a limited duration. The House discussion draft incorporates the limited authority suggested by the industry associations for FERC to respond to identified cybersecurity emergencies, and CEA supports the House discussion draft with the specific language options proposed by the associations.

CEA strongly supports the inclusion in the House discussion draft of a requirement that FERC consult with appropriate Canadian authorities before taking measures to address cybersecurity threats. Unlike the U.S. system, transmission is regulated in Canada primarily by provincial governmental authorities. Moreover, reliability standards are authorized and enforced by provincial governmental authorities. Consulting with the appropriate governmental authorities in the relevant provinces will help to ensure that actions taken by FERC are respectful of Canadian jurisdictional sovereignty and avoid unintended impacts on reliability and cross-

CEA

350 Sparks Street, suite 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - fax: (613) 230-9326 - info@canelect.ca

The voice of Canadian Electricity

350 rue Sparks, bureau 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - Téléc.: (613) 230-9326 - info@canelect.ca

ACE

La voix de l'électricité canadienne



border trade.¹ The absence of consultation between and among governmental authorities could further result in the elimination of, or reduction in, the sharing of critical cybersecurity information -- not a good result at a time when the sharing of information is becoming more and more important.²

CEA is also pleased that the House discussion draft makes clear that the NERC standard-setting process remains the appropriate vehicle for developing reliability standards, including cybersecurity standards. But CEA also recognizes that, given the nature of cybersecurity threats and the need to respond quickly, it may make sense to treat cybersecurity standards differently from operating and planning standards and to allow cybersecurity standards to be developed in a less public manner and in a way that allows for quick action to respond to ever-changing threats. In other words, NERC could establish an alternative standard setting process that would allow it to be more nimble in addressing cybersecurity issues. Such a process was suggested in a letter forwarded by NERC to NERC's Board of Trustees and Stakeholders on July 7, 2008. In that letter, NERC suggests the establishment of a task force to review "and where appropriate recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process." We would support NERC's efforts to establish a separate process for addressing cybersecurity issues. Importantly, this process would follow the NERC standard-setting model, thereby allowing for the development of cybersecurity standards that are respectful of Canadian jurisdictional sovereignty and allowing for the development of standards that can be approved by Canadian governmental authorities. In addition, CEA is encouraged by NERC's proposals to elevate the profile of its Critical Infrastructure Protection Program, to increase its

¹ The House discussion draft contains a requirement that consultation be subject to adequate protections to protect against disclosure, but FERC and the associations disagree over whether to use the term "inappropriate disclosure" or "public disclosure." For the sake of clarity and precision, CEA supports the use of the term "public disclosure."

² CEA also believes strongly that orders or measures to address known or imminent cyber-security threats must be accompanied by sufficient information sharing regarding the threat such that those implementing the order or measure can do so effectively.



Canadian Electricity Association
Association canadienne de l'électricité

www.canelect.ca

cybersecurity expertise and to better coordinate with governmental authorities. We believe that such steps would allow NERC to better respond to cybersecurity issues.

CEA appreciates this opportunity to provide this statement and would be happy to answer any questions that may arise during the hearing.

CEA

350 Sparks Street, suite 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - fax: (613) 230-9326 - info@canelect.ca

The voice of Canadian Electricity

350 rue Sparks, bureau 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - Téléc.: (613) 230-9326 - info@canelect.ca

ACE

La voix de l'électricité canadienne