



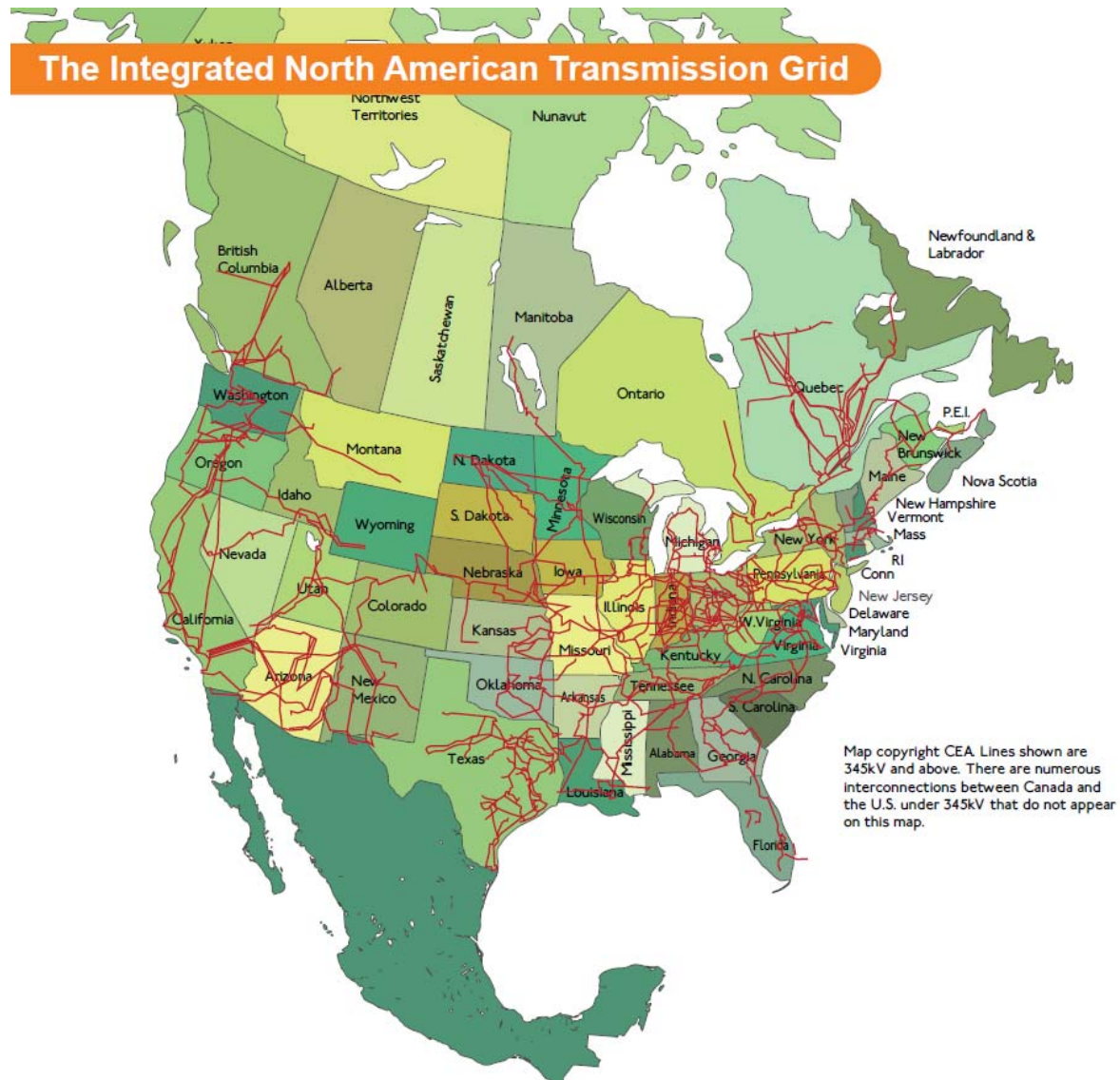
STATEMENT FOR THE RECORD OF  
THE CANADIAN ELECTRICITY ASSOCIATION  
BEFORE THE U.S. HOUSE HOMELAND SECURITY COMMITTEE  
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY,  
AND SCIENCE AND TECHNOLOGY  
HEARING ON  
“SECURING THE MODERN ELECTRIC GRID FROM PHYSICAL  
AND CYBER ATTACKS”

July 21, 2009

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 the appropriate actions that the U.S. Congress should take to protect the electric grid from cybersecurity threats and vulnerabilities. CEA’s members account for the majority of Canada’s installed generating capacity and high voltage transmission. In this statement, CEA explains the importance of taking cybersecurity actions in the U.S. that are mindful of the interconnected nature of the North American transmission grid and the importance of avoiding actions that could undermine the reliability of the transmission grid and impact cross-border trade. CEA further provides suggestions for this Subcommittee to consider before developing legislation to address physical and cyber security in the electricity sector. Specifically, CEA suggests that: (1) the North American Electric Reliability Corporation remain the primary body for addressing cybersecurity matters on the North American transmission grid; (2) any authority given to U.S. governmental authorities to address emergency situations be of a limited duration and be coordinated with Canadian governmental authorities; (3) consultation and information sharing between the U.S. and Canadian governmental authorities should be provided for in any legislation; and, (4) U.S. legislation should be respectful of Canadian sovereignty and jurisdiction.

## Background

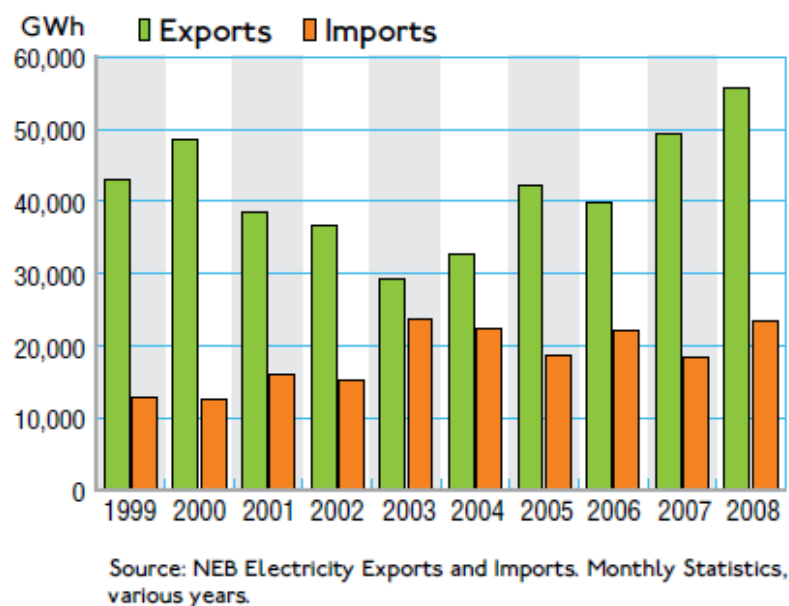
The electric transmission systems of U.S. and Canadian utilities are interconnected with one another at numerous points, forming a highly integrated North American transmission grid, as can be seen in the following map:



Of the 211,152 circuit miles of transmission lines greater than 200 kilovolts in North America, 46,499 circuit miles, or 22 percent, are located in Canada. This integration allows for cross-border trading, which facilitates 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.

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 1999 and 2008:



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 also 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 and mitigates risk by providing power during times of emergency outages or periods of high electricity demand.

Canadian utilities are part of and therefore critical to the energy security of the United States, and the reliability of the North American transmission grid.

### **Any Actions Taken in the U.S. to Address Cybersecurity on the Bulk-Power System Must be Coordinated With Canadian Governmental Authorities**

CEA recognizes the serious risks that cybersecurity threats and vulnerabilities present to the international grid. Nevertheless, CEA believes that any actions to address cybersecurity threats and vulnerabilities must be accomplished in a manner that recognizes the mutual interdependency of the interconnected Canada-U.S. transmission systems, and must not unintentionally imperil or downgrade reliability and erect barriers to cross-border trade.

The President of the United States recently directed a 60-day, comprehensive review to assess U.S. policies and structures for cybersecurity, and the result was the release of “Cyberspace Policy Review” on May 29, 2009. In the report, the White House concluded that “the United States needs a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat.” Understanding that the United States cannot act in a unilateral fashion, the report concluded:

The United States cannot succeed by acting in isolation, because cyberspace crosses geographic and jurisdictional boundaries. The United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations.

CEA supports the concept of cross-border cooperation between Canada and the U.S. to prevent cybersecurity attacks.

### **NERC is the Appropriate Standard-Setting Body for the North American Transmission Grid**

CEA believes that the best venue to address cybersecurity matters on the North American transmission grid 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 ensuring 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 the remand provision in the U.S. legislation, which is also incorporated into the processes for standards approval in a number of Canadian provinces 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 which would apply to the whole system, and that any 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.

NERC also has the ability to effectively incorporate the experiences and knowledge of the private sector in both the U.S. and Canada, which is especially important in this very technical industry. Any legislative directive must avoid placing the regulator in an operational role in terms of issuing detailed emergency procedures to address a present or imminent threat or vulnerability to electric system reliability. Such an approach would be consistent with the conclusions reached in “Cyberspace Policy Review” about the importance of a public-private partnership to address network security issues. As the President explained when the report was issued, “My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.”

Recognizing the need to better respond to cybersecurity challenges, NERC has recently established processes to allow for the expedited development of cybersecurity standards. NERC is developing approaches that 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. Importantly, this process follows 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 that NERC has elevated the profile of its Critical Infrastructure Protection Program, to increase its cybersecurity expertise and to better coordinate with governmental authorities. We believe such steps allow NERC to better respond to cybersecurity issues.

### **Considerations for U.S. Legislation**

CEA believes much of what needs to be done to address cybersecurity issues on the North American transmission grid can be accomplished through the NERC standards development process. Nevertheless, CEA recognizes that U.S. legislation may be necessary to address certain gaps in NERC authority. CEA has attached to this statement as an appendix a paper prepared by the major electric utility trade associations in Canada and the U.S. on the appropriate approach to take on cybersecurity. CEA also provides the following comments should this Subcommittee pursue a legislative strategy.

#### ***Authority to Take Action on an Emergency Basis***

CEA recognizes situations can arise requiring emergency actions to be taken immediately to protect the reliability of the bulk power system. To the extent that NERC does not have the

information or authority to respond to such an emergency situation, CEA agrees that governmental bodies should be able to respond expeditiously to ensure industry acts to protect the grid. In terms of U.S. governmental authority to respond to imminent cybersecurity threats, CEA understands the need for authority to address emergency situations, although we believe that such authority must be limited only to specific, credible and imminent cybersecurity emergencies, be of a limited duration, and be coordinated with Canadian governmental authorities.

### ***Consultation and Sharing of Information***

In any cybersecurity legislation, CEA strongly supports the inclusion of a requirement that the appropriate U.S. governmental agency 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 are respectful of Canadian jurisdictional sovereignty and avoid unintended impacts on reliability and cross-border trade. 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.<sup>1</sup>

---

<sup>1</sup> CEA also believes strongly that orders or measures to address known or imminent cybersecurity threats must be accompanied by sufficient information sharing regarding the threat such that those implementing the order or measure can do so effectively.

Consultation and information sharing is absent, for example, in H.R. 2195, a bill introduced by Homeland Security Chairman Bennie Thompson. The absence of a process for coordination between Canadian and U.S. governmental officials prior to any actions taken by FERC to address a cyber vulnerability or threat could undermine both reliability and security on the North American transmission grid. As noted in “Cyberspace Policy Review,” such coordination among governmental officials is critical to effectively addressing cybersecurity issues.

***Any U.S. Legislation Should be Respectful of Canadian Sovereignty and Jurisdiction***

In addition to the need for coordination between Canadian and U.S. governmental officials, this Subcommittee should also be mindful that U.S. legislation should avoid interfering with Canadian sovereignty and jurisdiction, which could undermine both cybersecurity and reliability. For example, in H.R. 2195, “critical electric infrastructure” is defined so broadly as to include Canadian systems and assets, since those systems and assets, if incapacitated or destroyed, could cause significant harm to the U.S. grid. Such a broad definition would, under this language, bring Canadian utilities within the scope of FERC authority under Section 224(e). Moreover, the Interim Measures authority under Section 224B would allow FERC to supplement, replace, or modify existing cybersecurity reliability standards approved by NERC. Since existing cybersecurity standards are in effect in the majority of Canadian provinces, the replacement of such standards in the U.S. by FERC could result in inconsistent reliability standards on the North American grid, thereby potentially undermining reliability and potentially making the system more vulnerable to a cyber attack. CEA therefore requests this Subcommittee to consider the impact that provisions in any proposed legislation could have on Canadian sovereignty and jurisdiction.



## **Need for Coordination Among Industry Sectors**

As a final matter, CEA is concerned with any legislative actions taken by Congress that fail to take into account the scope of the cybersecurity problem. As noted in “Cyberspace Policy Review,” cybersecurity affects all sectors and must be addressed in a comprehensive manner. CEA believes any cybersecurity bill would be greatly improved by requiring that the necessary information sharing and collaboration take place between governmental agencies and all the critical infrastructure sectors, not just electricity. A focus on just the electricity sector addresses only one piece of a much larger puzzle, and could, in fact, miss important elements to effectively addressing cybersecurity in the bulk power sector. The President’s report recognizes that the cybersecurity issue “transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective or authority to match the sweep of the problem.” Given the complexity of the cybersecurity problem, and the need for coordination on an international basis, CEA asks this Subcommittee to exercise caution before developing legislation to address cybersecurity in the electricity sector.

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

## APPENDIX



### **The North American Electric Power Industry's Top Priority is a Reliable and Secure Bulk Power System**

The stakeholders of the electric power industry continue to work closely and in partnership with governmental authorities at the federal, state/provincial and local levels in both the United States and Canada in order to maintain and improve upon the high level of reliability consumers expect. Cyber security is an important element of bulk power system reliability that the electric power industry takes very seriously.

#### **Electric Power Industry in Strong Partnership with Government**

The electric power industry works closely with various government agencies on bulk power system security. On an ongoing basis, we communicate and collaborate in the United States with the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC), and in Canada with the various federal and provincial authorities to gain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including cyber security standards. In addition, NERC has an “alert and advisory” procedure that provides the electric power industry with timely and actionable information to assure the continued reliability and security of the bulk power system.

#### **The Electric Power Industry Continuously Monitors and Acts Quickly to Ensure Bulk Power System Reliability and Security**

Every day, the electric power industry continuously monitors the bulk power system and mitigates the effects of transmission grid incidents – large and small. Consumers and government are rarely aware of these incidents because of the sector's advance planning and coordination activities which reflect the quick and often seamless response the sector takes to address reliability and security events. This response includes prevention and response/recovery strategies – both are equally important. The industry's strong track record on reliability and security continues as we work diligently to adhere to **mandatory** NERC reliability standards, which are approved by FERC, including standards that address cyber security.

### **NERC Flexible Standards Approval Processes Meet Majority of Grid Challenges**

NERC's industry-based and FERC-approved standards development process yields mandatory standards for the bulk power system that are clear, technically sound and enforceable, yet garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cyber-security, through consideration of the National Institute of Standards and Technology (NIST) framework for cyber-security, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also made important revisions to its standards development process by putting in place policies that allow, when necessary, for the confidential and expedient development of standards, including those related to cyber and physical security.

### **Emergency Cyber Situations Require an Expeditious and Efficient Approach**

If the federal government has actionable intelligence about an imminent threat to the bulk power system, the electric power industry is ready, willing and able to respond. We understand it may be necessary for government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards. In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. As FERC, NERC and the electric power industry relationships move forward and mature in the area of reliability and security, any disruption of this would be counterproductive.

### **Improved Electric Power Industry-Government Partnership with Better Information Flow**

In nearly all situations the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system. The electric power industry is fully committed to taking the needed steps to maintain and improve bulk power system reliability and security, and stands ready to work with Congress, FERC, other government agencies and NERC on these critical issues.

#### **Supporting Associations and Contacts:**

American Public Power Association  
Canadian Electricity Association  
Edison Electric Institute  
Electric Power Supply Association  
Electricity Consumers Resource Council  
Large Public Power Council  
National Association of Regulatory Utility Commissioners  
National Rural Electric Cooperative Association  
Transmission Access Policy Study Group

Joy Ditto	<a href="mailto:jditto@appanet.org">jditto@appanet.org</a>
Bonnie Suchman	<a href="mailto:bonnie.suchman@troutmansanders.com">bonnie.suchman@troutmansanders.com</a>
Scott Aaronson	<a href="mailto:saaronson@eei.org">saaronson@eei.org</a>
Con Lass	<a href="mailto:Class@epsa.org">Class@epsa.org</a>
John Anderson	<a href="mailto:janderson@elcon.org">janderson@elcon.org</a>
Jessica Matlock	<a href="mailto:jdmatlock@snopud.com">jdmatlock@snopud.com</a>
Charles Gray	<a href="mailto:cgray@naruc.org">cgray@naruc.org</a>
Laura M. Schepis	<a href="mailto:laura.schepis@nreca.coop">laura.schepis@nreca.coop</a>
Deborah Sliz	<a href="mailto:dsliz@morganmeguire.com">dsliz@morganmeguire.com</a>