



Canadian Commitment to Protecting the Integrated North American Electricity System Against Cyber and Other Security Threats and Vulnerabilities

With over thirty major transmission interconnections linking Canada and the United States, the continental electricity grid is a powerful driver of economic development and a focal point for health, safety and security matters on both sides of the border. Unfortunately, the electricity system can also be a strategic target for individuals and groups who seek to disrupt our way of life. The electricity industry needs to continually assess the protection of its critical electric systems and ensure responses to quickly recover from malicious attacks and technology-related failures.

As the generators, transmitters, distributors, operators, marketers and consumers of Canada's electricity supply, Canadian Electricity Association ("CEA") members are intimately familiar with the challenges involved in effectively responding to security incidents, threats and vulnerabilities. The Canadian electric utility industry has collaborated closely with Canadian provincial and federal authorities, U.S. government authorities and industry organizations for many years to share information and best practices and to develop industry-wide mandatory security standards through the North American Electric Reliability Corporation ("NERC"). Canadian utilities are committed to continuing to build upon industry practices and to further enhancing the protection of our critical electric systems.

Existing Industry Practices in Canada for Responding to Security Risks to the Grid

From a Canadian legal perspective, the issue of cyber security falls under the jurisdiction of both provincial and federal heads of government. The federal government has jurisdiction over international and interprovincial transmission lines, while the provincial governments have jurisdiction over generation facilities (excluding nuclear), intraprovincial transmission lines and distribution facilities. From a practical perspective, the activities required to protect the Canadian grid against security challenges are primarily executed through the mechanisms and legal authorities in place in each province, such as legislation, market rules, operating policies and emergency plans. The Canadian federal government also plays an important role in protecting the electricity grid against cyber security attacks, through its coordination with provincial authorities and the Canadian electricity industry.

As a general matter, provincial system operators have procedures in place for 24/7 monitoring and operations, and emergency procedures to address contingencies. Utilities and/or system operators have qualified individuals with appropriate security clearances and communications links with federal and provincial government authorities to enable the sharing of timely and actionable information to facilitate appropriate emergency responses. The following categories provide the general framework for assessing and responding to security matters:

- **Identify the security risk.** Across the provinces, measures are in place to enable the electricity industry to identify known or suspected incidents, threats and vulnerabilities to the electricity grid, in order to meet statutory obligations. At the federal level, the Canadian Cyber Incident Response Centre ("CCIRC") at Public Safety Canada monitors and identifies threats to critical infrastructure and notifies appropriate contacts. NERC also facilitates the identification of system threats and vulnerabilities across the North American bulk power system.

- **Receive and analyze data to assess the risk.** Following identification of potential security risks, the appropriate electric utilities and system operators receive the incident, threat or vulnerability information and analyze the data to assess the potential impacts to the electricity system. Each province has utilities and/or system operators with appropriate security clearances to thoroughly evaluate the potential security risks.
- **Direct Action.** In each province, electric utilities and/or system operators order and undertake the necessary actions to mitigate security risks to the electricity system. Consistent with the province’s individual market structure and reliability framework, utilities and system operators in Canada are also authorized to direct customers, market participants and/or asset owners to take specific action in order to safeguard grid reliability. Through approved NERC reliability standards, Reliability Coordinators have the authority to issue directives to asset owners and/or other reliability entities within their operating area.
- **Coordinate with Provincial Government.** From coast to coast, communication procedures are in place to enable electric utilities and system operators to inform and advise governmental authorities at the provincial level on any potential security risks at hand. Electric utilities and system operators execute their course of action in collaboration with these authorities.
- **Coordinate with Federal Government.** While provincial system operators bear principal responsibility for the operation of the electricity system in Canada, there is coordination between electric utilities and system operators with the Government of Canada on security matters through various agencies such as CCIRC, Canadian Security Intelligence Service (“CSIS”), Integrated Threat Assessment Centre (“ITAC”) and the Royal Canadian Mounted Police (“RCMP”).
- **Enforcement and Reporting.** Monitoring and enforcement measures are in place to ensure compliance with directives to address security issues, and to ensure that the security risks are effectively and thoroughly mitigated. Under certain approved critical infrastructure protection (“CIP”) standards, electric utilities and system operators in Canada are required to report on security matters to NERC, a Regional Entity, relevant governmental authority, and/or relevant local law enforcement agencies.

Importance of Coordination and Cooperation between Canadian and U.S. Governmental Authorities

CEA recognizes that Canadian entities cannot act in isolation from our international neighbors in assuring a secure grid. Efficient communication underpins the effective operation of critical electric infrastructure in Canada and the U.S. The delivery of electricity from generators to customers requires real-time, round-the-clock cooperation and coordination by electricity industry participants from all across North America. In the same way, when the interconnected electricity system is threatened, participants must be able to respond in a coordinated fashion in order to ensure the grid is properly protected and any security risk is properly mitigated.

Canadian provincial and federal governments presently share information on potential security risks with the Canadian electric industry. 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. Expedited sharing of critical infrastructure information between U.S. and Canadian governments, with the necessary mechanisms for dissemination and appropriate protections against improper disclosure, will help assure maintenance of a secure North American electricity grid.

