Canadian Electricity Association | Association canadienne de l'électricité

U.S. Department of Energy Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure

86 FR 21309

INTRODUCTION

The Canadian Electricity Association ("CEA") appreciates this opportunity to submit comments in response to the Department of Energy's ("DOE") Request for Information ("RFI") regarding preventing exploitation and attacks by foreign threats to the U.S. electric power system supply chain.

In the RFI, DOE seeks information on: (1) addressing pervasive and ongoing grid security risks requiring a comprehensive long-term strategy; and (2) addressing immediate threats to the electric grid through an expanded approach to Prohibition Orders ("PO") or similar actions that cover distribution facilities that serve Critical Defense Facilities, electric infrastructure serving other critical infrastructure sectors, and electric infrastructure enabling other critical functions.

CEA offers these comments in response to this proposal. They speak to issues regarding supply chain and cyber security generally, and in the spirit of the enduring value of cooperation between Canada and the U.S. on critical infrastructure security.

DESCRIPTION OF CEA

Founded in 1891, CEA is the national forum and voice of the evolving electricity business in Canada. CEA members generate, transmit, distribute and market electric energy to industrial, commercial and residential customers across Canada and into the U.S. every day. Our membership includes provincially-owned and investor-owned utilities, many of which are vertically-integrated; independent power producers; independent system operators; wholesale power marketers; and municipally-owned local distribution companies. Several CEA members own assets in the U.S.

CEA members are engaged in the buying and selling of electricity, ancillary services, and other energy and environmental products in markets across North America, including in Commission-approved regional transmission organization/independent system operator ("RTO/ISO") markets as registered participants.

CEA members include Balancing Authorities, Reliability Coordinators, Generator Owners and Operators, Transmission Owners and Operators, and other entities that are subject to reliability standards developed by the North American Electric Reliability Corporation ("NERC") that are adopted pursuant to the respective frameworks in place in Canadian jurisdictions governing electric reliability.

CEA members participate in other cross-border institutions and forums with their American counterparts that aim to ensure grid security, resilience and reliability, including the Electricity

Subsector Coordinating Council ("ESCC") and the Electricity Information Sharing and Analysis Center ("E-ISAC").

The Canada-U.S. Electricity Security Environment

The Relationship

Like their American counterparts, the Canadian electricity sector considers grid security, including supply chain security, a top priority.

There are more than 35 electric transmission interconnections between the Canadian and U.S. power systems, which together form a highly integrated North American grid and enable bi-directional electricity trade. In many cases, electricity companies from both sides of the border own and operate assets in both countries. Electric integration, trade, and cooperation have benefited both American and Canadian customers with a resilient, reliable, and secure grid for over 100 years.

This trade and integration form the backbone of a highly positive and mutually beneficial cross-border electricity relationship that provides economic, environmental, resilience and security benefits. It also contributes to affordable, and increasingly clean energy, for customers in both the U.S. and Canada. Further trade and integration assist both countries to reach their decarbonization goals in a resilient and affordable way.

The importance of this longstanding relationship is recognized by U.S. and Canadian governments. The recently announced *Roadmap for a Renewed U.S.-Canada Partnership ("Roadmap")* outlined opportunities to cooperate on electricity-related items, including "a coordinated approach to accelerating progress towards sustainable, resilient, and clean energy infrastructure, including encouraging the development of cross-border clean electricity transmission…"[1]

Underlying all of this is the imperative for ensuring secure electricity, and the value of likeminded countries and allies working on these issues. The *Roadmap* also noted that "Canada and the United States will increase cooperation to strengthen cybersecurity, and to confront foreign interference and disinformation. As part of their efforts to protect critical infrastructure in North America, the two countries will implement a Framework for Collaboration on Cybersecurity in the Energy Sector to enhance the security and resiliency of our cross-border energy infrastructure."[2]

Canada-U.S. Security Cooperation

Canadian and American BPS owners and operators understand that due to the interconnected nature of the North American electricity grid, its reliable and safe operation is a shared responsibility. CEA members participate in cross-border institutions and forums with their American counterparts that aim to ensure grid security, resilience and reliability, and which serve to support unity of effort and response.

---

[1] The White House. *Roadmap for a Renewed U.S.-Canada Partnership*. February 23, 2021.
[2] See above.

As noted above, the Canadian electricity sector includes owners, operators and users of the North American bulk power system that adhere to NERC standards, and who provide Critical Energy/Electric Infrastructure Information ("CEII") to NERC in compliance with mandatory reporting requirements. They also engage in NERC standards and guidance creation programs, and other forums in the electricity reliability and security space, working with U.S. counterparts to share expertise and information that serves to ensure electricity reliability and security.

CEA members, and Canadian government partners, participate in the ESCC and the E-ISAC. They also participate in cyber and physical mutual assistance programs with their American counterparts. Canadian utilities have sent hundreds of workers in recent years to assist with power restoration in the U.S. following hurricanes, Nor'easter storms, and wildfires in California. Mutual assistance has occurred even during COVID-19; for example, after Maine experienced a severe spring storm in April 2020, Hydro-Québec sent crews to assist. During the February 2021 severe weather events in the U.S., Manitoba Hydro and SaskPower provided support to MISO and SPP to help serve load.

The Canadian electricity sector and Canadian government also participate in major incident response exercises, including GridEx exercises, that simulate the likely cross-border impacts of coordinated attacks and natural disasters.

Current Efforts

The Canadian electricity sector, along with their American counterparts, understand the importance of supply chain and cyber security, and work to mitigate many different aspects of supply chain risk.

The manufacturer or foreign direct investment in a certain technology is just one of the many different aspects considered when evaluating risks. As technology advances and changes, including the advent of 5G technology, efforts to ensure continued security will have to continue to evolve as well.

The challenging cyber and supply chain security space that electricity companies must operate in is well described in the Canadian Centre for Cyber Security ("CCCS") National Cyber Threat Assessment ("NCTA"). CCCS is the Government of Canada's 'single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public'. The NCTA notes that the number of cyber threat actors are rising, and that they are becoming more sophisticated. Further, this is in the context of a rapidly evolving technology space.[3]

Activities to address evolving supply chain and cyber security risks include adhering to, or preparing to adhere to, relevant NERC CIP standards. NERC has supply chain and cyber standards currently in effect, under development, or which will be in effect, that address certain supply chain issues with which utilities are complying, or preparing to comply.

[3] Canadian Centre for Cyber Security. National Cyber Threat Assessment 2020.

As a general principle, while there may be certain cyber security and supply chain issues not addressed in currently effective CIP standards, CIP standards are just one of the many tools deployed to address security risks, including supply chain-related ones. Further, entities take many security actions that go beyond what is mandated in reliability standards to ensure protection against threats and vulnerabilities to cyber systems and to manage risk.

Indeed, both the National Institute of Standards and Technology Cyber Security Framework, which provides voluntary guidance for entities, and NERC CIP Reliability Standards, which are mandatory and enforceable, are valuable tools in addressing cyber risks. Information sharing through established forums such as the ESCC and the E-ISAC are important as well. The North American Transmission Forum is working with both utilities and suppliers on supply chain security issues, and, as noted above, NERC currently has various supply chain activities underway.

Of high importance as well are the strong partnerships built with government security and intelligence partners to identify, address, and share knowledge about threats, risks and vulnerabilities. In Canada, CEA members work closely in partnership with a wide range of partners, including Public Safety Canada, Natural Resources Canada, the Royal Canadian Mounted Police and the Canadian Centre for Cyber Security.

COMMENTS

The complex nature of supply chain and cyber security makes the need to have a variety of different tools to address threats, strong industry and government partnerships, and work with suppliers, all integral. Given the threats and the security landscape, continued conversations on these issues and efficient and appropriate action to address nearer and longer-term supply chain and cyber security issues are valuable. As DOE considers actions it can take, CEA would offer some of the following principles for consideration.

Stakeholder Consultation, Unity of Effort

CEA appreciates DOE's ongoing willingness to engage with industry and stakeholders on this issue, and encourages DOE to continue this approach. Supply chain security is a highly complex issue, with many diverse stakeholders involved. As such, CEA encourages DOE to continue to work closely with stakeholders on identifying the most effective and supportive actions that DOE can take to help the electricity sector further manage supply chain security risk. To assist with unity of effort, CEA would also encourage DOE to continue to seek opportunities to provide support to, or leverage, existing supply chain and cyber security efforts and information sharing forums such as the E-ISAC.

RD&D

The cybersecurity landscape is continuously shifting. As such, of high value is the facilitation and enabling of government, industry, and industry-government RD&D regarding cybersecurity tools and activities that can improve collective cybersecurity postures. This can help ensure continuous

improvement in the face of evolving threats. Partnership with Canada, in this regard, can help ensure we leverage our respective efforts in unity of effort as well.

Threat Intelligence Information Sharing

Information sharing between industry and government on supply chain security risk is highly valuable. Efforts should continue for government intelligence services to maintain and increase intelligence sharing on threats to the grid. It is essential, however, that information is shared with the private sector in even more timely and actionable ways. Examining ways to continue encouraging stronger and trusted industry and government partnerships to examine cyber threats within supply chains can serve to assist with the overall supply chain security posture.

Suppliers and CI Partners

Activity which encourages technology companies that serve the electricity sector to continue to improve their own cybersecurity practices, and to create more secure supply chains generally, is important. Electricity companies will continue to have effective cyber security protocols and procedures in place, and vendors which serve the sector should also be encouraged to have high cybersecurity expectations, and to continue to work in partnership with electricity companies and governments on these issues.

Areas to consider for sustainable and strengthened supply chain security in the longer-term could be the development of common security standards for vendors of key products and services used by the industry. Also of use could be actions that help electricity companies better and more easily understand if vendors, products, and services they use have relevant cybersecurity practices or protections in place. As we have seen with recent, public supply chain security compromises, threat actors will try to compromise any suppliers they can, including reputable ones. Deepening a culture of continuous improvement and strong security practices for all vendors with equipment/services serving critical infrastructure is important.

Also important is continued work with other CI sectors. For example, there would be value in the electricity and telecommunications industries continuing to work together to understand interdependencies and longer and shorter-term shared or systemic risks. This is especially valuable given the importance of the telecommunications industry to grid reliably at all voltage levels.

DOE, the FCC and relevant authorities in Canada could all help support the development of such efforts, which could include a review of all communication modalities in scope.

Implementation, Specificity and Prioritization

CEA encourages efforts to help enable utilities identify and mitigate specific, clearly identified risks in the most appropriate and flexible way.

Also encouraged is the use of a risk-based and flexible approach in any mitigation-oriented actions that DOE may consider taking. A risk-based approach allows for the tailoring necessary to accommodate

electricity entities' wide range of characteristics, such as geographic spread, service areas, populations served, and infrastructure, while also ensuring the effectiveness of outcomes.

Mitigation-oriented actions should also clearly and appropriately address a specific and identified issue, and should be based on engineering and intelligence-based prioritization, especially as entities may be required to make significant business decisions based on new intelligence or information.

Reliability

Given the specialized nature of some of the components that could be addressed in supply chain risk mitigation actions, CEA encourages DOE to ensure that reliability of the grid is also considered as part of any mitigation actions.

Financial Consideration

CEA encourages DOE to consider the potential cost implications of any rulemakings that may affect electric equipment markets. Equipment procurement is a costly and time-intensive process that already prioritizes safety highly among such other factors as reliability, availability and cost to ratepayers. CEA would caution DOE against unintended consequences that may result in trade-offs in other areas as the industry adapts to meet new requirements and procurement constraints.

Cross-Border Cooperation

Given the interconnectedness of the North American electricity system, as a general principle, CEA supports cooperation on security matters between Canadian and American bulk power system owners and operators and governmental authorities in a way that respects jurisdictional boundaries and considerations in both countries. Together we can leverage each others' efforts, and learn from each others' successes and challenges. CEA appreciates the communication between DOE, and the Canadian electricity sector and government partners thus far.

As such, CEA encourages DOE to continue to communicate and work in partnership with Canadian counterparts and the Canadian electricity industry. This includes working to facilitate responsible cross-border information sharing on supply chain security issues, and engaging in collective efforts to create a more secure and resilient North American electricity technology and infrastructure supply chain.

At the same time, governments should recognize that while Canadians and Americans both consider supply chain security a top priority, different jurisdictions may approach the issue in ways that are most appropriate to their unique realities

An area for deepened Canada-U.S. cooperation could include the development of a regularly updated joint view of systemic security risks facing the North American electricity industry, and our supporting critical infrastructure partners.

Using this shared view of systemic risk priorities, industry, other security partners and joint intelligence communities can align actionable intelligence that reduces overall risk and increases reliability.

Canadian Electricity Association | Association canadienne de l'électricité

Building off industry-led exercises like GridEx, relevant government authorities on both sides of the border (with industry partnership), along with NERC and the E-ISAC, could engage in coordinated exercises regarding shared risks, CI interdependencies or systemic risks, using the learnings to inform actions that improve our shared security postures.

CONCLUSION

CEA appreciates the opportunity to provide these comments. CEA respectfully requests consideration of the comments raised herein, and looks forward to continuing to work with the DOE to ensure the reliability, resilience, and security of the integrated North American grid.

June 2021

CEA CONTACT INFORMATION

Contact:
Francis Bradley
President & CEO
Canadian Electricity Association
275 Slater Street, Suite 1500
Ottawa, Ontario K1P 5H9
Canada
(613) 230-5027
Bradley@electricity.ca