Newfoundland Labrador

Government of Newfoundland and Labrador
Department of Natural Resources

November 1, 2019

[redacted]

Re: Your request for access to information under Part II of the *Access to Information and Protection of Privacy Act* (File # NR-209-2019)

On October 8, 2019, the Department of Natural Resources received your request for access to the following records/information:

> **RE: NR-167-2019 please provide a copy of the following note: Cyber security in the energy sector**

I am pleased to inform you that a decision has been made by the Department of Natural Resources, confirmed by the Deputy Minister, to provide access to the requested records. The responsive records are attached.

We are providing access to the most information possible but have made redactions in accordance with Sections 29(1)(a), 34(1)(a)(i) and 35(1)(d)(g) of ATIPPA, 2015 as follows:

29. (1)(a) The head of a public body may refuse to disclose to an applicant information that would reveal advice, proposals, recommendations, analyses or policy options developed by or for a public body or minister;

34. (1)(a)(i) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to harm the conduct by the government of the province of relations between the government and the following or their agencies: the government of Canada or a province;

35. (1)(d) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose information, the disclosure of which could reasonably be expected to result in the premature disclosure of a proposal or project or in significant loss or gain to a third party.

35. (1)(g) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose information, the disclosure of which could reasonably be expected to prejudice the financial or economic interest of the government of the province or a public body.

As set out in section 42 of the Act you may ask the Information and Privacy Commissioner to review the department's decision to provide access to the requested information. A request to the Commissioner must be made in writing within 15 business days of the date of this letter or within a longer period that may be allowed by the Commissioner. Your request should identify your concerns with the department's response and why you are requesting a review.

The request for review may be addressed to the Information and Privacy Commissioner is as follows:

Office of the Information and Privacy Commissioner
2 Canada Drive
P.O. Box 13004, Stn. A
St. John's, NL. A1B 3V8

Telephone: (709) 729-6309
Toll-Free: 1-877-729-6309
Facsimile: (709) 729-6500

Pursuant to section 52 of the Act, you may also appeal directly to the Supreme Court Trial Division within 15 business days after receiving the department's decision.

Please be advised that responsive records will be published following a 72 hour period after the response is sent electronically to you or five business days in the case where records are mailed to you. It is the goal to have the responsive records posted to the Completed Access to Information Requests website within one business day following the applicable period of time. Please note that requests for personal information will not be posted online.

For further details about how an access to information request is processed, please refer to the Access to Information Policy and Procedures Manual at http://www.atipp.gov.nl.ca/info/index.html.

If you have any questions, please feel free to contact me at 709-729-0463 or rhynes@gov.nl.ca.

Sincerely,

Rod Hynes

Rod Hynes
ATIPP Coordinator

New England Governors/Eastern Canadian Premiers NEG/ECP Briefing Book
Background Note – Cyber Security in the Energy Sector
Department of Natural Resources

Title: Cyber Security in the Energy Sector

Issue: [redacted] S.29.1.a S.34.1.a.i This note provides an overview of cyber security as it pertains to the energy sector.

Background and Current Status:

- Cyber security of critical energy infrastructure requires close cooperation among jurisdictions because such infrastructure is largely provincially regulated, and in some cases owned by provincial Crown corporations. Canada's critical energy infrastructure includes oil and gas pipeline systems, electric grids, nuclear plants, etc.

- Natural Resources Canada (NRCan) collaborates with provinces, territories and industry to address growing cyber threats to critical energy infrastructure.

- In June 2018, NRCan released the National Cyber Security Strategy identifying the leadership role of the Government of Canada. The Strategy conveys the importance of strengthening communication and collaboration with provincial and territorial partners to share best practices, lessons learned, technical training, and threat information to ensure the security of Canada's critical infrastructure systems.

- [redacted] S.29.1.a S.34.1.a.i

Analysis:

- [redacted] S.29.1.a S.34.1.a.i

- [redacted]
- [redacted]

S.29.1.a
S.34.1.a.i
S.35.1.d
S.35.1.g

- Cybersecurity standards such as those developed by the North American Reliability Corporation ("NERC") for the bulk transmission system continue to evolve. For utilities that operate below the bulk transmission high voltage level that is not under the direction of NERC, other standards have been developed at the provincial and state level.

- In their respective annual capital plans filed with the PUB, Newfoundland and Labrador Hydro (NLH) and Newfoundland Power both list projects related to the use and maintenance of security software tools and hardware designed to mitigate threats to computer systems and networks. Maintaining the security of the power system in this way is critically important to keep the power system operating and to protect customer information.

- NLH is sensitive to cybersecurity and is working to minimize risks from potential threats. NLH has undertaken audits of critical infrastructure consistent with NERC standards, initiated an internal security group, secured insurance for cyber threats and has upgraded business security software.

- NLH's Operational Technology Group has responsibility for computer software and cyber protection in its system control centre and is implementing technology such as firewalls and other software protections. While NLH is not required to adopt the documentation and administrative measures for NERC standards, it is adhering to best practices with respect to operations. NLH officials participate in cyber security working groups with the Canadian Electricity Association (CEA). In the past year, software protections have been extended into various switch yards such as the one at Soldier's Pond.

- Newfoundland Power has developed a Cybersecurity Risk Management Plan that includes assessing approximately 200 cybersecurity controls and a two-year cybersecurity roadmap.

Prepared by/Reviewed by: Y. Khan/R. Bates/K. Bradbury/
Approval:

August 29, 2019