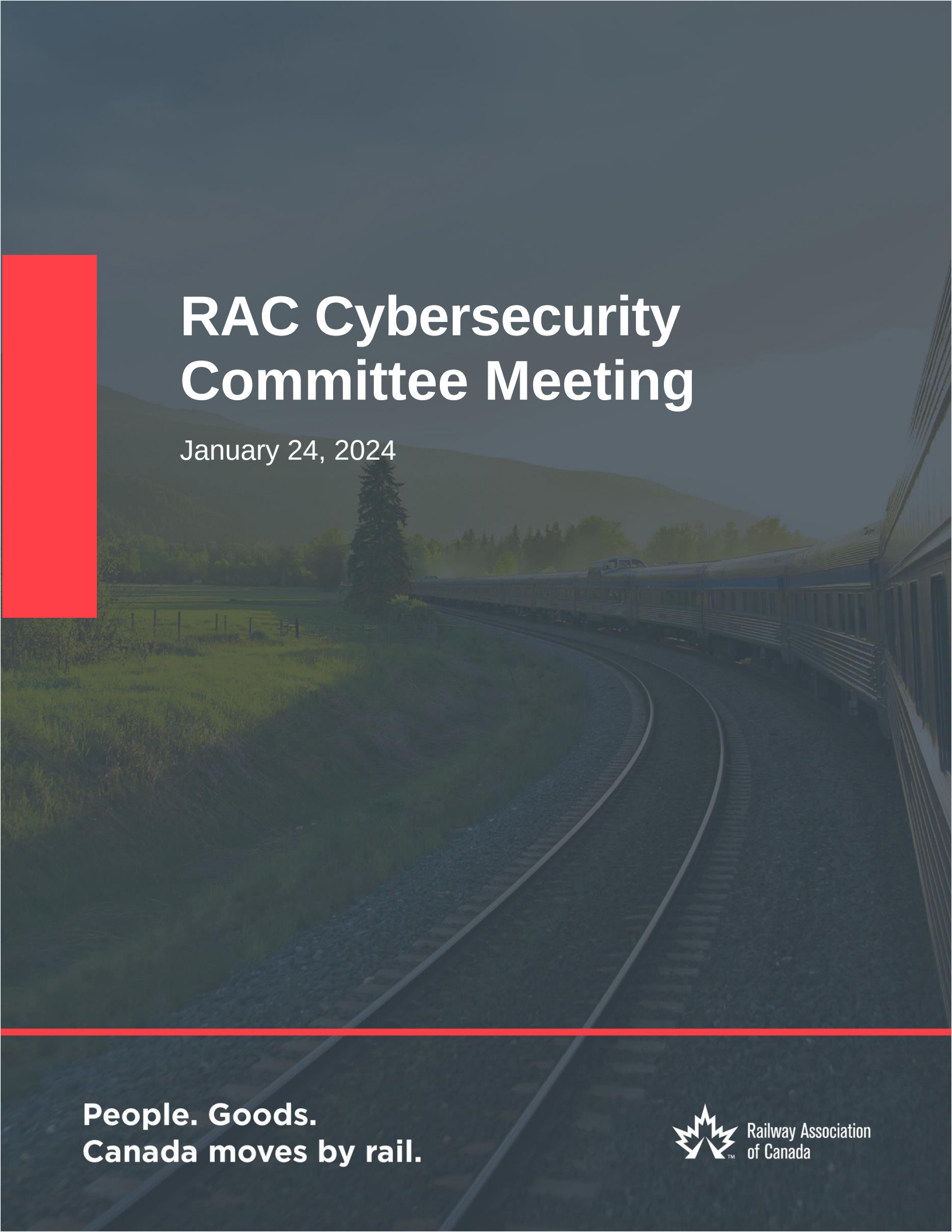

RAC Cybersecurity Committee Meeting

January 24, 2024

People. Goods.
Canada moves by rail.

Railway Association of Canada

Railway Association of Canada

Competition Law Compliance Policy

STATEMENT

The RAC is committed to compliance with all **competition laws** applicable in Canada, including Canada's ***Competition Act***.
Under the leadership of its Board of Directors, the RAC carries out its activities in strict compliance with all **competition laws**, provides guidance to its committees and its employees on how to comply with these laws, and promotes with them the importance and value to the RAC of complying with them.
The RAC Corporate Secretary ensures that RAC, its committees and its staff are familiar and comply with this policy.

COMPETITION LAW

Competition laws are designed to maintain and encourage competition in the marketplace. Non-compliance with the **competition laws** relating to improper coordination among competitors could constitute a criminal offence to which significant fines and prison terms can be attached, and for which significant damages can be awarded in private lawsuits, including large class actions.
RAC is a forum for railway members to exchange information and views on the railway sector. Particularly because RAC is an association that represents most of the players in the rail sector in Canada, including many that compete with one another, any activity it conducts must be in strict accordance with the **competition laws**, and avoid even the perception of possible improper conduct.

PROHIBITED ACTIVITIES

Due to the presence of multiple competing entities in RAC, any activity, including discussions or agreements that relate, directly or indirectly, to the following "**Prohibited Topics**" are strictly prohibited:

- ÿ Prices (rates) charged to shippers for services provided by members of the RAC
- ÿ Prices (costs) paid to suppliers for services provided to members of the RAC
- ÿ Any other conditions associated with services provided to shippers or received from suppliers of RAC members, including discounts, rebates, etc. and level of service provisions
- ÿ Customer or territory allocation
- ÿ Limitation of supply of services provided by RAC members to their customers

GUIDANCE

Any activity, including discussions or agreements that could even remotely be construed as relating to the above Prohibited Topics, cannot take place at the RAC or any of its committees or any meeting organized or attended by RAC staff, or otherwise among RAC members.
To ensure compliance with these rules, when meeting, members of a RAC committee or of the Board of Directors must:

- ÿ Have a pre-set agenda and take minutes, recording resolutions adopted and summarizing the essentials of conversations that took place.
- ÿ Limit themselves to issues identified on the agenda, except if circumstances call for other issues to be addressed, in which case careful notes of the additional issues discussed must be recorded.
- ÿ If any participant believes that Prohibited Topics have been raised or discussed, they must advise all participants of their concern and any discussion relating to that issue be ceased immediately pending legal advice.
- ÿ Require legal advice if any issue to be discussed might cause the members to believe that **competition laws** could be infringed.
- ÿ Suspend or even postpone to a later date discussions on such issues if legal advice cannot be sought in a timely manner.

Staff of the RAC shall in their duties ensure the confidentiality of information brought to their attention by members, avoid conflict of interest or situations that would discredit the RAC, unless doing so could violate the **competition laws**.

Updated May 3, 2021

Railway Association of Canada

RAC CYBER SECURITY COMMITTEE MEETING

January 24, 2024
13:00 – 14:30 (ET)

Microsoft Teams Meeting
Click here to join the meeting

AGENDA

	SCHEDULE	DISCUSSION LEADER	TIME
1.	**Welcome to Order** Welcome all participants.	**All**	**13:00**
2.	**Competition Compliance Statement** – Forward Statement	**RAC**	**13:05**
3.	**Introductions** Participants introduce themselves.	**All**	**13:10**
4.	**Committee Chair and Vice-Chair** Appointment of Chair and selection of Vice-Chair for the Committee	**All**	**13:20**
5.	**Terms of Reference Discussion**	**All**	**13:30**»
6.	**Bill C-26 Response** General discussion and determination of creation of work group to address the Bill.	**Vaughn Hazen**	**13:30**»

D **Decision Required**
» ***Supporting material***

Railway Association of Canada

Cyber Security Committee

Borhani, Alex
Sr. Director and Deputy CISO
CSX Corporation
Alex_Borhani@csx.com

Chung, Mike
Managing Director, Enterprise Security
CPKC
(913) 449 9427
Michael.Chung@cpkcr.com

De Benetti, Enzo
Consultant, RAC Spectrum & Telecommunications
Railway Association of Canada
(438) 455 7236
edebenetti@railcan.ca

Dewar, Janna
Senior Manager, Cybersecurity
VIA Rail Canada Inc.
Janna_Dewar@viarail.ca

Gill, Jessie
Manager, Systems Technical Services
West Coast Express Ltd.
(778) 879 2107
JESSIE_GILL@BCRTC.BC.CA

Hazen, Vaughn
Assistant Vice-President and Chief Information Security Officer
CN
(514) 399 4953
Vaughn.Hazen@cn.ca

He, Biying
Director - IT Security,Risk, Compliance & Resilience
West Coast Express Ltd.
Biying.He@translink.ca

Hislop, Rick
IT Security Manager
Great Canadian Railtour Company Ltd.
(604) 606 7200
rhislop@rockymountaineer.com

McLeod, Adrian
Senior Communication and Security Engineer
Ontario Northland Transportation Commission
(705) 472 4500
Adrian.McLeod@ontarionorthland.ca

Du Perron, François
Lead Advisor, Cybersecurity and Networks - CFR
VIA Rail Canada Inc.
(514) 871 6201
Francois_DuPerron@viarail.ca

Singh, Malwinder
Security Operations Specialist
CPKC
(403) 888 8388
Malwinder.Singh@cpkcr.com

St.John, Janet
Director, Cybersecurity
Association of American Railroads
(202) 639 2221
jstjohn@aar.org

Sukhera, Fawad
Security Analyst, Security Operation Center | I&T
CN
(514) 399 8245
Fawad.Sukhera@cn.ca

Sul, Douglas
Senior Manager, Operational Technology
CPKC
(204) 218 8826
Douglas.Sul@cpkcr.com

Railway Association of Canada

The Railway Association of Canada
Cybersecurity Committee
Terms of Reference

Name

This committee shall be known as the RAC Cybersecurity Committee.

General Mandate

The general mandate for this committee is to provide RAC members a forum:

- For the identification and assessment of industry cybersecurity concerns.
- To monitor and advise on new or proposed changes to cybersecurity-related legislation or regulation and evaluating the impact of such changes on the industry.
- To identify and recommend opportunities for cybersecurity improvements within the industry.
- To facilitate and coordinate cybersecurity concerns and activities between freight and passenger members
- Collaborate with the federal and provincial governments to enhance the rail cybersecurity posture to prevent, mitigate, respond to and recover from potential terrorist or major cybersecurity incidents.

The Cybersecurity Committee will monitor, analyze, and provide reports and recommendations to the RAC Safety Committee on matters within the scope of its mandate. The Cybersecurity Committee will serve as a focal point for sharing of ideas, technology, best practices, and new initiatives that provide positive improvements in cybersecurity within the industry.

The Cybersecurity Committee may establish Working Groups to study specific cybersecurity incidents or issues and deliver on targeted project objectives.

Each Working Group will develop its own terms of reference and elect a Chair. Working Groups will report to and be governed by the decisions of the Cybersecurity Committee.

Committee Responsibilities & Guidelines

- Monitor, assess and report findings and recommendations to SOMC on issues emanating from within the committee's mandate.

- Research and report on issues assigned to the Committee by the membership.

- Foster an open environment of sharing cybersecurity program strategies and successes, new technologies and procedures, incidents and exercises, threat assessments where appropriate and generally spearhead ideas that enhance the development of all member company's cybersecurity initiatives.

- Ensure that regulators overseeing railway cybersecurity and other agencies with an interest in cybersecurity are made sufficiently aware of railway operations and

cybersecurity activities. The Cybersecurity Committee will promote voluntary approaches for cybersecurity management rather than prescriptive regulatory approaches.

- Review, assess, develop, and implement appropriate broad industry strategies that promote the cybersecurity interests of RAC members. These could include industry cybersecurity best practices and guidelines, cybersecurity training packages, presentations, and other activities.

- Act as the managing entity for the various cybersecurity-related activities in which RAC is engaged as well as assessing and reviewing proposed regulatory actions related to cybersecurity, including Bill C-26.

- Monitor industry cybersecurity intelligence (as appropriate and reasonable for this level of participation), trends, incidents and other related cybersecurity issues and identify improvement opportunities.

- Liaise as required with other organizations involved in the promotion of cybersecurity and threat assessment / risk management in the industry, including AAR.

Officers

There shall be a Chair and Vice-Chair, elected by the Cybersecurity Committee from its membership. Their terms of office shall normally be of two years, which can be renewed. It is recommended that these officers represent freight and passenger interests respectively.

An officer from the RAC will be appointed to the Cybersecurity Committee as a member and will assist in the management of the Cybersecurity Committee's activities and act as the Secretary.

Duties of Officers

The Chair shall be responsible for the general supervision of the affairs of the Cybersecurity Committee, preside at meetings and be empowered to call special meetings as conditions warrant. The Chair will act as the Cybersecurity Committee spokesperson to SOMC. The Vice-Chair shall perform duties of the Chair whenever the Chair is unable to perform the duties of his/her office.

The Secretary will record the events of the proceedings including but not limited to discussion topics, resolutions, action items and responsibilities. The Secretary will draft minutes of the meeting and forward them to the Chair for approval/distribution within 21 calendar days.

Membership

Membership is open to the RAC, RAC member companies, and the AAR. Persons shall be nominated by their respective companies and shall serve until the person notifies the Chair of his/her resignation. Membership will be of special interest to those with responsibilities in the function of corporate cybersecurity, regulatory affairs, railway operations and risk management.

A member who is unable to attend a meeting, should send a representative who shall be counted in determining a quorum and be permitted to vote in place of the regular member.

Decisions will be made on a consensus basis with recommendations being made to the Security Committee that reflect this consensus.

Meetings

The Cybersecurity Committee shall meet on an quarterly basis or on a schedule to be determined by the committee. Special meetings may be called in response to significant developments. Meetings may be held by telephone, video conference or any other means allowing people to communicate and make decisions on a real time basis, at the discretion of the members.

Quorum

The quorum at meetings of the Cybersecurity Committee is five members. One member should be from CN, and one from CP. The following three railway categories should also be represented: passenger (intercity, commuter or tourist), shortline and US carrier. A RAC or an AAR member can be considered as a railway member in the shortline or US carrier categories for quorum purposes.

Reporting Authority

The Cybersecurity Committee will report to the SOMC. The Cybersecurity Committee will liaise with other RAC committees and working groups on matters which are of mutual interest.

Railway Association of Canada Bill C-26 Backgrounder

Confidential and privileged draft

Prepared by Nadia Effendi, Dan Michaluk and Shane Morganstein of BLG

On June 14, 2022, the federal government introduced Bill C-26 – a new cybersecurity law that, if passed, will enact the *Critical Cyber Systems Protection Act* (the "CCSPA") and impose a range of new obligations on federally regulated railways. The new obligations will require railways to establish, implement and maintain cyber security programs that meet stipulated requirements and report cyber incidents "immediately." Bill C-26 will also provide the government, including the Minister of Transport, with additional powers over railways, including the power to issue binding directions and compliance orders and to pursue significant administrative monetary penalties for non-compliance.

This backgrounder describes the major features of the proposed new law with a view to supporting discussion amongst the members of the Railway Association of Canada.

The context

Bill C-26 follows commitments made in the government's National Cyber Security Strategy and National Cyber Security Action Plan to secure critical infrastructure and provide support to Canadian critical infrastructure owners and operators.

The federal government launched its Strategy and Action Plan in 2018, but the threat has since heightened. Notorious incidents like the Colonial Pipelines ransomware incident that affected the United States in May 2021 have led Canada's allies to take action to address the threat posed to critical infrastructure. Industry groups have continued to urge government to better secure Canadian critical infrastructure and supply chains.

In the rail sector, the 2018 *Railway Safety Act* Review (the "2018 RSA Review") recommended that Transport Canada clarify the requirements under the *Railway Safety Act* and supporting instruments to better support cyber security, leading government to commit to consider legislating change. The 2018 RSA Review cited cyber attacks on rail systems:

> *Cyber attacks, which include hacking, infection with malware or viruses and physical attacks also pose a threat to rail safety.271 High-profile examples of cyber attacks*

affecting rail operations include a 2008 case in Poland where a teenage boy modified a TV remote to trigger rail switches, causing four trains to derail, as well as a case in 2011 where railway signals in the northwestern US were disrupted for two days by hackers who attacked a railway company's computers.

Also, in the United States, in December 2021, the Transportation Security Administration (the "TSA") issued ***Security Directive 1580-21-01*** to impose accountability, incident response and vulnerability assessment obligations on freight railroad carriers, which were expanded in October 2022 in *Security Directive 1580/82-2022-01*.

The Canadian government's stated objectives in introducing Bill C-26 are to "address longstanding gaps" in its ability to protect systems and services of national importance and to establish a broad regulatory framework enabling the federal government to:

- designate services and systems that are vital to national security or public safety in Canada, as well as the operators or classes of operators responsible for their protection;
- ensure that designated operators are protecting the cyber systems that underpin Canada's critical infrastructure;
- ensure that cyber incidents that meet or exceed a specific threshold are reported;
- compel action by organizations in response to an identified cyber security threat or vulnerability; and
- ensure a consistent cross-sectoral approach to cyber security in response to the growing interdependency of cyber systems.

Application to railways and scope of application

Bill C-26 is intended to apply to the rail sector and other federally regulated sectors, with rail sector oversight to be assigned to the Minster of Transport.[1]

[1] Section 2, "appropriate regulator" and "regulator." Bill C-26 gives the executive the power to designate the Minister of Transport as a regulator responsible of Bill C-26 oversight, presumably, so the Minister can be assigned responsibility for oversight of railways and other transportation system operators.

Bill C-26 does not impose duties on railways directly. Rather, it gives the executive the power to order federally regulated railways to be "designated operators" – the persons who will bear the primary duties under the new legislation.[2]

Although application to railways is not yet certain, federally regulated railways are likely to be designated given the government's prior commitments following the 2018 RSA Review and given they carry on a business in respect of a "transportation [system] that [is] within the legislative authority of Parliament", one of six "vital" services and systems identified by the proposed legislation.[3]

The legislative and regulatory framework in Bill C-26 will only apply to "critical cyber systems." A "cyber system" is a set of "interdependent digital services, technologies, assets or facilities"[4] and a "critical cyber system" is:

> *a cyber system that, if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system.[5] [emphasis added]*

Should Bill C-26 be passed, railways will need to identify their cyber systems and assess their criticality, bearing in mind that the words "could affect" establish a low criticality threshold. In its current form, Bill C-26 likely encompasses control systems and a wide range of other railway systems.

Key designated operator duties

Bill C-26 will impose five key duties on railways. We briefly describe each below.

1. Duty to establish, implement and maintain a cyber security program (a "CSP")

Railways will be required to establish a cyber security program that addresses the cyber risk to each critical cyber security system they manage.

[2] Section 7.
[3] Section 2, "vital service" and "vital system" and Schedule I.
[4] Section 2, "cyber system."
[5] Section 2, "critical cyber system." The Transportation Security Administration definition in Security Directive 1580/82-2022-01is comparable, encompassing any system that, if compromised, "could result in operational disruption."

A CSP must set out, in accordance with any regulation to be passed, reasonable steps to:

- identify and manage organizational cyber security risks, including risks relating to the railway's supply chain and use of third-party products and services;
- protect critical cyber systems from being compromised;
- detect cyber security incidents affecting critical systems; and
- minimize the impact of any cyber security incidents.[6]

Railways will be required to file CSPs with the Minister of Transport, to review their CSPs periodically and to notify their regulator whether or not any amendments arose from a review.[7]

The duty to file a first CSP will arise 90 days from railways' designation unless the Minister of Transport grants an extension.[8] The duty to commence a review will be set by regulation (or otherwise fall on a CSP's anniversary date), and reviews must ordinarily conclude within 60 days from the date of commencement.[9]

Railways will have a duty to "implement" and "maintain" their CSPs by taking all reasonable steps that they contain.[10] In other words, railways will be statutorily bound to the commitments they make in their CSPs, subject to amendments that arise out of a periodic review.

It appears that railways will be permitted to prioritize and schedule their risk mitigation commitments, with the exception of risk mitigation commitments relating to supply chain risks. Bill C-26 prioritizes supply chain risks by stipulating that designated organizations must take steps to mitigate such risks "as soon as" they are identified.[11]

2. Duty to report cyber security incidents

The CCSPA will require railways to "immediately report a cyber security incident in respect of its critical systems."[12] This "report" is to be sent to the Communications Security Establishment (the "CSE"),[13] and immediately followed by a "notification" and, upon request, a copy of the

[6] Section 9(1).
[7] Sections 10 and 13.
[8] Sections 10 and 11.
[9] Section 13.
[10] Section 12.
[11] Section 15.
[12] Section 17.
[13] The CSE is Canada's signals intelligence agency, whose mandate includes a cyber security component.

report to the regulator.[14] Railways must make reports and notifications in accordance with any requirements set out in regulations.[15]

A "cyber security incident" is any incident (includes act, omission or circumstance) which interferes or may interfere with (a) the continuity or security of a vital service or system, or (b) the confidentiality, integrity or availability of the critical cyber system.[16] This would include, for example, a ransomware attack with the potential to affect a passenger railway's booking system.

For those familiar with privacy breach reporting, cyber incident reporting under the CCSPA will be very different. Indeed, reporting will be based on interference with critical systems or services, not to the information contained in systems or records. Even containment action that involves shutting down information technology services will trigger interference (and therefore reporting), whether not the threat actors have access or stolen any confidential data at all.

Reporting is also required based on the mere potential for interference. Without an amendment, railways may struggle to distinguish between the many immaterial "cyber events" – ***e.g.***, alerts and false positive reports – that they identify from cyber incidents that must be reported. Railways may also rush to report and over-report given the Bill does not contemplate a period of assessment or investigation.[17]

3. Duty to comply with cyber security directions

Bill C-26 will give the government the power to make binding directions "for the purpose of protecting a critical cyber system."[18] Directions will set out "measures to be taken" along with any conditions and a time period for compliance.[19] Railways will be notified of directions to which they are bound, and will not be able to be found to have contravened the direction unless it is proven that at the time of the contravention they had been notified.[20] Further, railways must

[14] Section 18.
[15] Sections 17 and 18.
[16] Section 2, "cyber security incident."
[17] This said, the Transportation Security Administration definition the United States railway security directives is comparable, and stipulates that the definition of security incident includes events that are under investigation or evaluation.
[18] Section 20(1).
[19] Section 21(1).
[20] Section 22(2).

keep the existence of directions and their content confidential except as necessary for compliance purposes.[21]

The government's power to issue directions is broad, and not expressly constrained by pre-conditions such as necessity or reasonableness. There is no requirement to consult with railways about potential operational impact or other concerns prior to or after issuing a direction nor will directions be subject to the same vetting process that applies to regulations under the *Statutory Instruments Act*.[22]

Railways may seek judicial review of directions by applying to the Federal Court. However, the hearing may be subject to certain restrictions on procedural fairness by virtue of national security issues. Indeed, at any time during the judicial review, the Minister of Public Safety and Emergency Preparedness can request that the hearing occur in the absence of the public and of the applicants and their counsel and the Federal Court must acquiesce to the request if it believes that the disclosure of evidence or other information could be injurious to international relations, national defence or national security or endanger the safety of any person.[23] If the Federal Court hears the matter *ex parte* and *in camera*, it must nonetheless provide the applicant with an opportunity to be heard and ensure that the applicant is provided with a summary of the evidence that enables them to be reasonably informed.[24] There is no statutory provision for a security-cleared special advocate with a mandate to protect the interests of designated organizations.[25]

4. Duty to keep certain records

Railways will be required to keep records respecting:

- any steps taken to implement their cyber security program;
- every cyber security incident reported under section 17;
- any steps taken under section 15 to mitigate any supply-chain or third-party risks;
- any measures taken to implement a cyber security direction; and

[21] Section 22(2)
[22] Section 22(1).
[23] Section 145(1)(a).
[24] Section 145(1)(c).
[25] Secrecy has been identified as a key flaw in the Bill C-26 proposed amendments to the *Telecommunications Act* by Christopher Parsons of the Citizen's Lab. See *Cybersecurity Will Not Thrive in Darkness A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act*.

- any other matter prescribed by the regulations.[26]

Railways will be required to keep records in Canada at a place prescribed by regulation or, if no place is prescribed, at their place of business.[27] They will also be required to keep records in the manner and for the period determined by the appropriate regulator unless another manner or period is prescribed by regulation.[28]

5. Duty to notify of material changes

Railways will be required to notify the Minister of Transport of certain material changes, including (i) any material change in their ownership or control and (ii) any material change in their supply chain or their use of third-party products and services.[29]

Information sharing and confidentiality

Bill C-26 provides for government use and disclosure of the information provided by designated organizations and, to protect the security and business interests of designated organizations, deems certain information confidential.

"Confidential information" means any information obtained under the CCSPA in respect of a critical cyber system that:

- concerns a vulnerability of any designated operator's critical cyber system or the methods used to protect that system and that is consistently treated as confidential by the designated operator;
- if disclosed could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a designated operator; or
- if disclosed could reasonably be expected to interfere with contractual or other negotiations of a designated operator.[30]

[26] Section 30(1).
[27] Section 30(2)
[28] *Ibid.*
[29] Section 14.
[30] Section 2, "confidential information."

While providing for the protection of confidential information, Bill C-26 expressly authorizes extensive information sharing. Specifically, the Bill:

- permits regulators to share confidential information with the Communications Security Establishment (the CSE) regarding a designated operator's CSP to seek "advice, guidance or services" from the CSE;[31]
- permits regulators to share confidential information with the Minister of Public Safety and Security for any purpose related to the CCSPA;[32]
- permits the sharing of confidential information within the federal government for the purpose of making, amending or revoking a cyber security direction;[33]
- permits the Minister of Public Safety and Security to share confidential information with provincial governments and agencies under "an agreement or arrangement" that the Minister of Public Safety and Security deems to be sufficiently protective;[34] and
- permits the Minister of Public Safety and Security to exchange information (other than confidential information) with foreign states and international organizations.

In addition to these express allowances, the CCSPA's confidentiality prohibition does not apply to disclosures of confidential information "necessary for any purpose related to the protection of vital services, vital systems or critical cyber systems."[35]

Enforcement

Bill C-26 provides the Minister of Transport with inspection and audit powers and the power to make compliance orders. The compliance order scheme in the CSSPA supports expeditious order making, with minimal procedural requirements. The Minister:

- may order compliance (to stop doing something or take any measure that is necessary in order to comply) without consultation and based only on a "[belief] on reasonable grounds that there is or is likely to be a contravention";[36]

[31] Section 16.
[32] Section 28.
[33] Section 23.
[34] Section 27(2).
[35] Section 26(1) (which introduces a significant ambiguity).
[36] Section 82(1). This is less constrained than the analogous power 32(3) of the *Railway Safety Act*, which is conditioned on an "immediate threat to safe railway operations."

- may stipulate the time within which and the manner in which an affected designated operator may seek a review of the order;[37] and
- will review their own orders on the request of the designated operator.[38]

If the Minister does not respond to a request for review within 90 days, Bill C-26 will deem the order to be confirmed.[39]

The Minister may also impose administrative momentary penalties ("AMPs") of up to $15 million per contravention.[40] The procedure for imposing penalties is similar to that set out in the *Railway Safety Act*.[41] Designated operators will have 30 days to pay or request a review by the Transportation Appeal Tribunal upon receiving a notice of violation.[42] A single member of the Tribunal will conduct a review hearing in which the Minister has the burden of proving a contravention, following which either party may appeal the matter to an appeal panel.[43]

The CSSPA will deem a failure to report a cyber incident and a failure to notify a regulator of a cyber incident to be an offence punishable on summary conviction.[44] It will also deem a number other acts and omissions to be offences punishable on summary conviction or via indictment. These include:

- a failure to establish a compliant CSP;
- a failure to take the reasonable steps set out in the program;
- a failure to mitigate supply chain risks as soon as they are identified;
- a failure to comply with a direction; and
- disclosing the existence of a direction except as necessary to comply.[45]

[37] Section 82(2).
[38] Section 84.
[39] Section 85(2).
[40] Sections 91 and 127.
[41] See sections 40.1 to 40.22.
[42] Section 129(2).
[43] Sections 130 to 132.
[44] Section 136(1).
[45] Section 137.

Bill C-26 stipulates that due diligence will not be a defence to any failure to establish a compliant CSP nor any failure to mitigate supply chain risks as soon as they are identified.[46]

Conclusion

Canadian rail safety regulation is not new, and railways are likely to have developed cyber security controls as part of their safety management systems. However, the advent of a framework by which government can establish new substantive obligations and that provides for meaningful regulatory scrutiny of railway cyber security is very significant.

While the form of regulation in Bill C-26 will likely evolve, there is little doubt that railways will soon face strict cyber security requirements. Railways who have not developed reasonably mature cyber security programs should invest in improvements beginning now.

The form in which the government is proceeding with its critical infrastructure cyber security policy also raises concerns. The CSSPA is framework legislation with very limited substance or clear guidance. Railways can assess only the high-level requirements relating to CSP establishment, implementation and maintenance, with the required substance of CSPs likely to be dealt with in detail by regulation. More specifically:

- the cyber incident reporting requirement is broad, leading to concerns about burdensome Ministry of Transport oversight and interference;
- of similar concern, the Ministry's power to inspect and to make compliance orders is very broad;
- exposure to cyber security directions raises significant concerns about potential operational burdens, yet Bill C-26 features few procedural safeguards and, given the prospect of secret hearings, transparency is limited;
- Bill C-26 provides for substantial administrative monetary penalties, yet removes a due diligence defence for certain offences.

Government is legitimately concerned with the need for a responsive regime that protects sensitive information from adversaries, though there are legitimate and important questions for

[46] Section 141. The comparable statutory defence in section 42 of the ***Railway Safety Act*** is complete, we note. The limitation in section 141 raises a ***Charter***-compliance issue we would be pleased to analyze.

railways and other critical infrastructure owners and operators to consider about whether Bill C-26 strikes an appropriate balance.

November 7, 2022

Railway Association of Canada

October 4, 2023

ENSURING RAILWAYS CAN CONTINUE DELIVERING FOR CANADA: RECOMMENDATIONS TO IMPROVE BILL C-26

A submission to the House Standing Committee on Public Safety and National Security

OVERVIEW

The Railway Association of Canada (**"RAC"**) provides this submission to the House of Commons Standing Committee on Public Safety and National Security in support of its study of Bill C-26, ***An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*** (**"Bill C-26"**).[1]

Rail is the backbone of Canada's transportation system. Hardworking railroaders transport more than $350 billion in goods and tens of millions of passengers each year. A recent study found that rail contributes $17.6 billion to Canada's GDP, generates $7.2 billion in tax revenue, supports 182,000 jobs, and lifts incomes by $10.1 billion.[2] Railways move Canada.

Cybersecurity is a strategic priority for the RAC and its members. It is linked to safety, the fluidity of supply chains, and economic growth.

Railways have a shared interest in preventing cyberterrorism and industrial espionage, and in protecting Canadian consumers and supply chains. The RAC supports the broadly stated goals of Bill C-26, but the Bill in its current form has several important flaws.

FLAWS IN BILL C-26

1. **Words matter:** Bill C-26 as currently drafted contains ***vague, undefined language*** that creates scope confusion and could lead to over-reporting low-risk incidents and a crippling lack of prioritization. Overly prescriptive (vs. risk-based) regulation can lead to unintended consequences and operational practicality issues.

2. **Misalignment can disrupt integrated cross-border supply chains:** Canadian railways that operate in the United States have spent several years working with the U.S. Transportation Security Administration (**"TSA"**) to develop definitions and interpretations of similar regulations by our largest 'Five Eyes' partner. Not aligning to these regulations risks creating inconsistent and incompatible systems that ***disrupt vital cross-border trade***.

3. **Partial data, flawed decisions:** Ministerial directives based on incomplete and untested early data could be problematic and ***paralyze effective responses*** to cybersecurity incidents. The proposed Bill also contains harsher monetary penalties than currently exist in other legislation and regulation governing Canada's railways.

RECOMMENDED CHANGES

1. **Clarify and carefully define** language in legislation and regulation so railways and government alike are focused on what matters and able to respond to serious incidents in timely, effective ways.

2. **Align** cybersecurity obligations on Canadian railways to match the scope, definitions, and interpretations of TSA Security Directive 1580/82-2022-01[3], released in October 2022. This will allow for faster implementation, prevent supply chain slowdowns, and protect cross-

border trade with our closest neighbour, most important ally, and largest trading partner.

3. **Focus** on risk-based rather than prescriptive regulations. Account for and elevate risks based on probability and impact. If or when cybersecurity incidents occur, responders' operational agility is critical.

    a. At minimum, railways in question should be meaningfully consulted before any ministerial directive is issued (and this should be established by statute).

    b. A focused approach would:

        i. Eliminate provisions that elevate supply chain risks above all others in railways' cybersecurity plans to avoid mis-prioritization.

        ii. Clarify accountabilities and timelines for the establishment and implementation of cyber security programs.

        iii. Amend duty to report to within 72 hours so the true nature of a risk or threat is known.

        iv. Amend threshold for reporting incidents to embed a two-factor risk model, considering probability and impact.

        v. Ensure that security sensitive information does not need to be filed with government but would instead be available for review on site so that appropriate government officials can be informed while providing better protection for the information by leaving it in the hands of the operator.

        vi. Clarify that breach-related exchanges, information shared about cybersecurity programs, and any other legally required information exchanged with government officials are excluded from Access to Information requests.

        vii. Remove constraint on due diligence defence to avoid confusion and unclear liability.

        viii. Align compliance order powers to those in the ***Railway Safety Act***, including reducing the proposed maximum AMP of $15 million to $250,000.

CONCLUSION

Canada's railways are deeply committed to protecting critical infrastructure (physical and cyber).

The convergence of operational technology, information technologies, and the Internet of Things (OT-IT-IoT) presents both opportunity and challenge, including risks to keep rail networks secure.

All Canadians have a stake in ensuring we find effective and practical solutions to pressing cybersecurity challenges.

Fixing the issues with Bill C-26 will allow railways to stay focused on preventative measures and rapid responses when rare issues arise.

Sincerely,

Marc Brazeau
President
Railway Association of Canada

ABOUT RAC

The Railway Association of Canada (**"RAC"**) represents close to 60 freight and passenger railway companies. The RAC also counts a growing number of industrial railways and railway supply companies in its associate membership. As part of the fifth largest rail network in the world, RAC members are the backbone of Canada's transportation system.

---

[1] Online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading.

[2] Online: https://www.railcan.ca/wp-content/uploads/2020/05/Moving-People-Products-and-the-Economy-the-Economic-footprint-of-Canadas-rail-industry.pdf.

[3] Online: https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf.

Borden Ladner Gervais LLP
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto ON M5H 4E3
Canada
T 416-367-6000
F 416-367-6749
blg.com

Borden Ladner Gervais

Memorandum

Date: December 2, 2022

To:	Caroline Healey
From:	Dan Michaluk
Client/Matter No:	033678.000009
Subject:	Meeting re Bill C-26

Attendees

BLG: Dan Michaluk, Shane Morganstein

CN: Eric Harvey, Amir Ashuri, Graham Nasby, Vaughn Hazen, Melissa Cotton

CP: Nathan Cato

RAC: Marc Brazeau, Chris Day, Caroline Healey

Discussion of scope issues

- Important to align scope with US scope
    - Articulated in TSA directives
- "critical cyber systems"
    - Definition vague, not necessarily in conflict with US scope but should check
    - Preference is to achieve alignment via statutory amendment

Possible RAC position

-Amend definition of critical cyber system to ensure scope of regulation is aligned with scope of US regulation

Discussion of duty to establish CSP

- There will be a binding obligation to implement CSP
    - Need accountabilities
    - Need timelines
- Significant concern with treating supply chain risks differently than all other risks
    - Requirement is strict and not risk-based
    - There are "low risk" supply chain risks, as with any risk
    - "Risks are risks"
    - (Effectively) deeming all supply risks to will lead to mis-prioritization

Possible RAC position

-Eliminate provisions that elevate supply chain risk above all other cyber risks (and develop an alternative/step down position)

Discussion of duty to report cyber incidents

- What?
    - "May" is vague and could be more clear, else risk of over reporting low-risk incidents (to the detriment of the Minister)
    - Interest in advocating for a two factor risk model – probability and impact
    - There are low impact cyber risks – e.g. train delayed for five minutes
    - Interest in advocating for 72 hours (and seeming openness to same)
    - Earlier reports create accuracy risks

Possible RAC position

-Amend threshold for reporting to embed a two-factor risk model – probability and impact

-Amend timing to 72 hours

Discussion of duty to comply with directions

- Major concern/priority concern
- RSA enforcement is far more simple (physical risk scenarios are the norm)
- At a minimum should be a duty to consult (and consultation is the norm in RSA enforcement)

Possible RAC position

-Develop an alternative to proposed power that addresses the risk of problematic directions, including (at a minimum) a duty to consult prior to issuing a directive

-Seek to qualify the confidentiality protections associated with judicial review application to enhance fairness and transparency

Discussion of duty to keep records (minimal discussion)

Discussion of duty to notify of material change

- Concerns with breadth of supply chain requirement noted
- (At least) refinement of risk based threshold required

Possible RAC position

-If the obligation to notify of material change in supply chains/use of third-party products is not eliminated (per the above), advocate for a clear and higher risk-based threshold for notification

Discussion of confidentiality protection (minimal discussion)

Possible RAC position

-Argue for narrowing, including by implementing a fully class based (rather than harms based) definition of "confidential information" and addressing the problematic and arguably broad allowance in section 26(1)

Enforcement

- Rhetorically, what justified a broader power to order compliance than under the RSA?
- Concern about inviting adversarial and punitive enforcement
- Concern about constraint on due diligence defence – does it apply to both fines and AMPs?
    - Answer: strangely, the defence is only constrained in respect of offences (for certain contraventions).

Possible RAC position

-Seek to align the compliance order power with the RSA compliance order power

-Seek to narrow the range of offences to correspond with more serious contraventions

-Seek the removal of the due diligence constraint