



RAC Cybersecurity Committee Meeting

April 11, 2024

People. Goods.
Canada moves by rail.



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:

- ☐ Prices (rates) charged to shippers for services provided by members of the RAC
- ☐ Prices (costs) paid to suppliers for services provided to members of the RAC
- ☐ 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
- ☐ Customer or territory allocation
- ☐ 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:

- ☐ Have a pre-set agenda and take minutes, recording resolutions adopted and summarizing the essentials of conversations that took place.
- ☐ 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.
- ☐ 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.
- ☐ Require legal advice if any issue to be discussed might cause the members to believe that **competition laws** could be infringed.
- ☐ 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

RAC CYBERSECURITY COMMITTEE MEETING

**April 11, 2024
13:00 – 14:00 (ET)**

Microsoft Teams Meeting
[Click here to join the meeting](#)

AGENDA

SCHEDULE	DISCUSSION LEADER	TIME
1. Welcome, Call to Order and Roll Call	Vaughn Hazen (Chair)	13:00
1.1 Competition Law Compliance Policy – Forward Statement	Enzo De Benetti	13:05
2. Approval of Meeting Minutes (January 24, 2024)	Vaughn Hazen	13:10» D
3. Update from Cybersecurity Working Group	Enzo De Benetti	13:15
4. General Discussion	All	13:30
5. Miscellaneous / Adjournment	Vaughn Hazen	14:00
D	Decision Required	
»	<i>Supporting material</i>	

**RAC CYBERSECURITY COMMITTEE MEETING
DRAFT MINUTES 24-01
Virtual Meeting
January 24, 2024; 13:00 HOURS (ET)**

In Attendance

Brianna Bowman (RAC)
Enzo De Benetti (RAC)
Jana Dewar (VIA)
François Du Perron (VIA)
Jessie Gill (WCE)
Vaughn Hazen (CN)
Rick Hislop (Rocky Mountaineer)
Adrian McLeod (ONTC)
Malwinder Singh (CPKC)
Janet St. John (AAR)
Fawad Sukhera (CN)

Regrets

Alex Borhani (CSX)
Mike Chung (CPKC)
Biyang He (WCE)
Douglas Sul (CPKC)

1. Welcome & Introductions

Mr. De Benetti called the meeting to order in accordance with the Railway Association of Canada (RAC) bylaws and read the Competition Law Compliance Policy – Forward statement.

2. Committee Chair and Vice-Chair

RESOLUTION: It was moved by the committee to nominate Vaughn Hazen, CN as Chair of the *RAC Cyber Security Committee*, and 2 years thereafter as per the Terms of Reference, effective until January 24, 2026. *Officers: There shall be a Chair and Vice Chair elected by its membership. The terms of office shall normally be 2 years.*

RESOLUTION: It was moved by the committee to nominate Janna Dewar, VIA as Vice-Chair of the *RAC Cyber Security Committee* and 2 years thereafter as per the Terms of Reference, effective until January 24, 2026. *Officers: There shall be a Chair and Vice Chair elected by its membership. The terms of office shall normally be 2 years.*

3. Terms of Reference Discussion

The Terms of Reference were reviewed and accepted. The committee agreed to meet quarterly.

4. Bill C-26 Response

The committee reviewed the draft RAC response to Bill C-26. No changes or additions were noted. The committee agreed that a working group focused on Bill C-26 would be pertinent. The working group will be made up of the following people: Jana Dewar (VIA), Rick Hislop (Rocky Mountaineer), Jessie Gill (WCE), Fawad Sukhera (CN) and Enzo De Benetti (RAC). The working group will establish a mission statement and a scope of work and report back to the larger Cybersecurity Committee at its next meeting in April 2024.

5. Next meeting

A Doodle Poll will be sent after this meeting to decide the date for a meeting in April.

The meeting was adjourned at 13:46 ET.

Action Items	Lead	Status
1. Circulate meeting minutes	Brianna Bowman	Completed
2. Send doodle poll for next committee meeting in April.	Brianna Bowman	Completed
3. Send doodle poll to schedule working group meeting	Brianna Bowman	Completed
4. Status of RAC response to Bill C-26	Enzo De Benetti	Completed

Cyber Security Committee

Hazen, Vaughn

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

Chair**Dewar, Janna**

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

Vice Chair**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

Gill, Jessie

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

**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 a 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 CPKC. 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.