HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

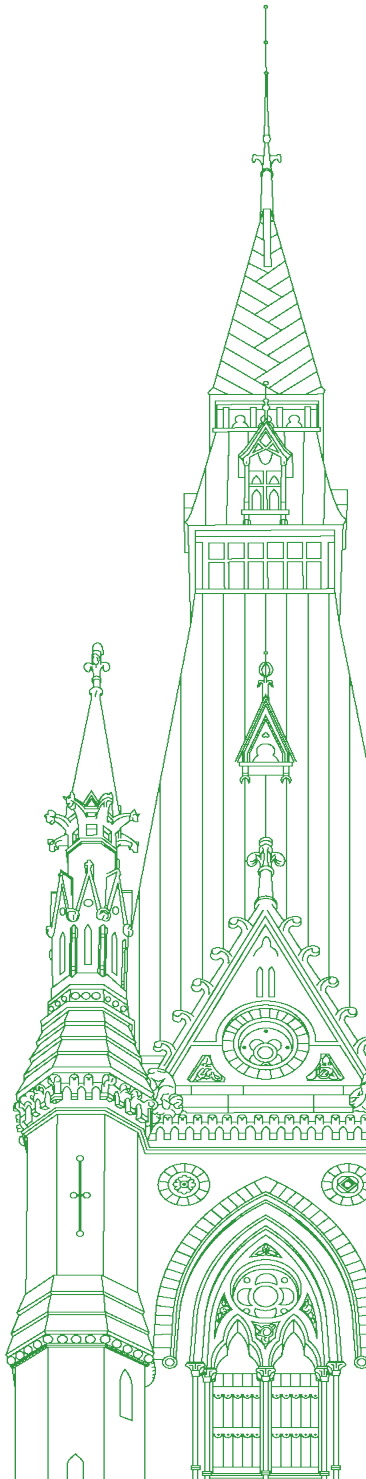
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 093

Thursday, February 8, 2024



Chair: Mr. Heath MacDonald

Standing Committee on Public Safety and National Security

Thursday, February 8, 2024

● (0815)

[*English*]

The Chair (Mr. Heath MacDonald (Malpeque, Lib.)): I call this meeting to order.

Welcome to meeting number 93 of the House of Commons Standing Committee on Public Safety and National Security. Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and remotely using the Zoom application.

I would like to make a few comments for the benefit of witnesses and members.

Please wait until I recognize you by name before speaking.

To prevent disruptive audio feedback incidents during our meeting, we kindly ask that all participants keep their earpieces away from any microphone. Audio feedback incidents can seriously injure interpreters and disrupt our proceedings.

All comments should be addressed through the chair.

Pursuant to the order of reference of Monday, March 27, 2023, the committee resumes its study of Bill C-26, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts.

I would like to welcome our witnesses for the first panel.

From Blackberry, we have John de Boer, senior director, government affairs and public policy, Canada. From the Canadian Cyber Threat Exchange, we have Jennifer Quaid, executive director. From Electricity Canada, we have Francis Bradley, president and chief executive officer.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions.

Welcome to all of you.

I invite Mr. de Boer to make an opening statement, please.

Dr. John de Boer (Senior Director, Government Affairs and Public Policy, Canada, BlackBerry): Thank you, Mr. Chair.

On behalf of BlackBerry, I'm delighted to speak with committee members today.

For over 35 years, BlackBerry has invented and built trusted solutions to give people, governments and businesses the ability to stay secure and productive.

Today, we are a leader in cybersecurity software and services. We protect more than 500 million systems worldwide. Our customers include all G7 governments, NATO, 45 of the Fortune 100 companies, nine of the top 10 global banks and numerous critical infrastructure entities.

Critical infrastructure is a prime target for cybercriminals and state-sponsored actors. At BlackBerry, we know this first-hand. Between September and December 2023, we stopped more than 5.2 million cyber-attacks, and 62% of those targeted critical infrastructure.

Just yesterday, the Canadian Centre for Cyber Security, along with Five Eyes partners, issued an advisory confirming that PRC state-sponsored cyber-actors had compromised entities across multiple critical infrastructure sectors in the United States, including communications, energy, transportation, and water and waste-water infrastructure.

The director of the U.S. Cybersecurity and Infrastructure Security Agency fears that this is “likely the tip of the iceberg.” Canada's cyber centre assesses that, “should U.S. infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration.”

In addition to delivering essential services, critical infrastructure entities house large amounts of sensitive information, including intellectual property, technical designs and personal information that are attractive targets for cyber-threat actors.

Currently, apart from PIPEDA-related obligations, Canada has no legislation in place to govern, much less obligate, critical infrastructure entities to report, prepare for and prevent cybersecurity incidents.

The critical cyber systems protection act will help drive necessary investment to improve cyber resilience and help ensure that critical infrastructure entities can operate through disruption and recover rapidly.

Stepping back to a larger comparative picture, Canada is falling behind our G7 peers in cybersecurity. U.S. and European governments have already taken regulatory measures that raise the bar on critical infrastructure cybersecurity. In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which requires covered critical infrastructure entities to report cybersecurity incidents to government within 72 hours, and ransomware payments within 24 hours. In October 2022, the European Union approved legislation requiring operators of essential services to implement baseline cybersecurity measures and notify national authorities of serious cybersecurity events within 72 hours.

Canada is currently out of step with our closest allies on cybersecurity. This legislation will help close the gap. Cyber-incident reporting will help government and private sector entities quickly share relevant information, warn and protect other potential victims and rapidly deploy resources and assistance to contain damage from cyber-incidents.

As the committee considers this legislation, BlackBerry would like to offer three recommendations to strengthen the law.

First, harmonize cyber-incident reporting requirements with our key allies, notably the United States. Doing so will help minimize the unnecessary burden on reporting entities and help ensure that the resources of entities facing an incident are dedicated to mitigating the effects of cyber-incidents. Second, provide guarantees that cyber-information reported by the covered entities is protected from liability, based on the information they report. Third, ensure that entities covered by the cyber-incident reporting requirements are not punished by punitive measures for good-faith efforts to comply with the law.

In conclusion, this law will help close the gap in our country's ability to prevent cyber-attacks, improve situational awareness, foster rapid and effective response and help create a culture of proactive, prevention-first cybersecurity at scale.

BlackBerry stands ready to work with this committee to strengthen Canada's cyber-resilience.

● (0820)

Thank you.

The Chair: Thank you, Mr. de Boer.

Ms. Quaid, you're next, please.

Ms. Jennifer Quaid (Executive Director, Canadian Cyber Threat Exchange): Good morning, Mr. Chair.

Thank you, all.

I have the honour of being here today representing the Canadian Cyber Threat Exchange, which is an organization created by Canadian companies to provide a safe environment for members to share cyber-threat information and collaborate by sharing best practices and ideas. The goal is to build cyber-resilience and create a stronger economic environment for all. With 170 members, representing 15 sectors and more than 1.5 million employees, our members are actively sharing cyber-threat information to help build awareness and resilience in others and to prevent breaches, as well as the corresponding need to report.

Many of our members represent the critical infrastructure sectors impacted by this legislation, while others make up their supply chain. Many of them are small and medium businesses, like so much of the Canadian economy.

I applaud the government for focusing its attention on creating legislation that will help strengthen Canada's critical infrastructure sector. I believe that with a few small modifications, there is an opportunity with this legislation to do more to support resilience among Canadian businesses and to strengthen the Canadian economy beyond the confines of the six critical infrastructure sectors referenced.

Others have spoken eloquently about privacy issues and about the real risks of attributing liability to our CISOs. All are very good points, which we support.

I want to talk about three cost-effective suggestions that are easily implemented and will have a significant impact on cyber-resilience throughout Canada.

First, the legislation should be amended to include language that encourages all organizations to voluntarily share cyber-threat information and to collaborate with others to build resilience. This can be done with the addition of language in the preamble and two small related changes. I'd be happy to provide the committee with some of the proposed text later.

The second change is to make membership in a Canadian cyber-threat information-sharing association an allowable expense for government programs. For example, Canada's industrial and technological benefits policy does not permit membership in an organization as an allowable inclusion. This change would incentivize companies to participate in a sharing and collaborative organization to raise their cyber-awareness and resilience in an ongoing way. It would be a small change with a significant impact at no cost to the government.

Third, this legislation requires only specified organizations to share cyber-incident information with their regulators or with the government. We have an opportunity here to create a legal environment that enables all companies, including those specified, to share information beyond what they are required to by law. The CCTX has Canadian members and Canadian companies whose American extensions are currently sharing information in the U.S. that they can't share in Canada because they are not protected by legislation. They are concerned about civil liability if they voluntarily share information that could help others prevent an incident.

The objective of Bill C-26 is to prevent further cyber-incidents. Mandated reporting of incidents is not enough. It will not protect enough organizations quickly enough. By adding protection from civil liability, this legislation could fix that. You could enable companies to share beyond what is strictly necessary to become compliant and improve the cybersecurity and resilience of the economy as a whole in a cost-effective, meaningful way. Without this protection, critical information will continue to be shared with organizations outside of Canada.

In creating and supporting the CCTX, Canada's business community continuously demonstrates its willingness and desire to share cyber-threat information and to share its expertise and experience to support Canadian businesses. Help it do more. Enable it to do more. If enacted as part of this legislation, these three changes will ensure a more secure supply chain for critical infrastructure, which is the focus of this bill, and for all Canadian businesses, large and small.

Thank you.

● (0825)

The Chair: Thank you, Ms. Quaid. You're right on time.

Mr. Bradley, you'll go next, please.

[*Translation*]

Mr. Francis Bradley (President and Chief Executive Officer, Electricity Canada): Thank you, Mr. Chair.

I'm CEO of Electricity Canada, formerly known as the Canadian Electricity Association. Our members are companies that generate, transmit and distribute electricity in every province and territory in Canada.

My comments today will focus on part 2 of Bill C-26, which enacts the Critical Cyber Systems Protection Act.

[*English*]

Before I proceed, I want to acknowledge the efforts of federal departments in drafting Bill C-26 and the time spent engaging stakeholders over the past two years. The problems that the bill is trying to solve are hard ones, with lots of moving pieces and far-reaching implications against the backdrop of a constantly evolving threat landscape.

While I commend the efforts, I must add my voice to the witnesses you've already heard from who emphasized the importance of getting this legislation right. While we acknowledge the urgency to pass this type of legislation, it is crucial to carefully consider amendments and resist the pressure to rush through the review the bill.

Mandatory security requirements can help strengthen our overall security posture, but the approach taken by Bill C-26 risks having the opposite effect, adding very little security to our sector and redundantly adding additional layers of regulatory requirements. Today, I will highlight three areas where the legislation falls short and requires improvement.

First, the bill must align with existing regulatory frameworks. The electricity sector is unique in that the assets targeted by Bill C-26 are already regulated by the North American Electric Reliability Corporation, or NERC. This poses a risk of regulatory conflicts, increases the burden on operators and introduces compliance confusion and ambiguity, ultimately impeding the goal of Bill C-26 to enhance the safety of our critical system.

A witness last week recommended that the bill should take a risk-based approach and impose fewer requirements on those with already strong cybersecurity programs. Under this approach, mature organizations could spend more resources on incident prevention instead of compliance activities, and regulators could better focus their time on high-risk operators. Given our sector's strong security posture and the existing NERC standards, we feel that a risk-based approach to Bill C-26 would be a step in the right direction.

Another area needing improvement in the bill is its reporting requirements. The reference to the immediate reporting of cyber-incidents should be revised. Reporting obligations should not divert critical infrastructure operators from their response and recovery efforts during and post incident. Reporting requirements should be well defined and consistent and have a reporting timeline that is flexible enough to allow the effective use of limited resources during incident response and recovery.

Still on the topic of reporting requirements, the goals of the legislation would be better served if it included legal protection for operators. Safe harbour provisions are an important part of promoting information sharing between industry and government, ensuring the successful implementation of the new reporting requirements and promoting voluntary information sharing.

The final aspect I wish to address is the unintended impact of the bill on the existing industry-government collaboration. Imposing mandatory requirements may create a chilling effect on the industry's relationship with government departments and agencies. Without appropriate safeguards, operators would likely receive legal advice to share just enough information to comply with the act and nothing more.

This is counterproductive to the goals of the legislation, but there are a couple of things you could do to mitigate those risks. First, put clear limits on how the government can use the information collected by way of this act. Several provisions in the bill would allow for information sharing among a range of persons and entities, and it does not explicitly limit how recipients use the collected information.

Second, the cyber centre should be carved out from the legislation and exempt from obligations to report information obtained by way of the act to other entities. Critical infrastructure operators currently enjoy a positive and collaborative relationship with the cyber centre. This is grounded in the confidence that the cyber centre does not disclose operators' information to regulators, enforcement agencies or other departments. Protecting the cyber centre from information-sharing obligations is crucial to maintaining this collaborative relationship.

● (0830)

[*Translation*]

Many other aspects of Bill C-26 also deserve our attention, but my time's up for this morning.

However, I encourage you to take a look at our brief, which contains 14 recommendations on how to improve Bill C-26.

Thank you.

[*English*]

The Chair: Thank you, Mr. Bradley.

I thank all of you.

We're going to move right into the rounds of questions. The first round will be six minutes, and we're starting with Mr. Lloyd, please.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

I want to thank all the witnesses for coming today, and for their testimony. We're taking notes, and we'll be taking everything you've said under advisement in our consideration of this bill.

Going forward, though, we do have another urgent issue that we're facing in this country, and it is the issue of auto theft. In the interests of allowing this committee to continue working on Bill C-26, but also to walk and chew gum at the same time and deal with the urgent issue of auto thefts in this country, I plan to be moving my motion that I put on notice at the last committee meeting to discuss. However, given that there have been some discussions with the other parties present, we have come forward with proposed amendments to this motion so that we can program this committee to work simultaneously on Bill C-26 while also working on the very important issue of auto theft.

We know that in 2022, the latest year that auto theft insurance statistics were made available, $1.2 billion in auto theft claims were made. We know that over 100,000 vehicles were stolen in Canada last year. This is a growing issue. It has increased, year over year, 50% in the provinces of Ontario and Quebec. It's a cross-Canada issue. Alberta is the third highest on the auto theft issue. This is a very important issue in my riding and I am very concerned.

We do need education to help people know what tools are available to them to help protect their vehicles from auto theft. However, at the same time, if the federal government does not take action to secure our ports and to put these repeat offenders behind bars, I fear that we are going to see an increase in the brazenness of these criminal acts, including violence committed against our citizens, if we don't take action to immediately put a chokehold on this unprecedented flow of Canadians' vehicles out of, particularly, the port of Montreal.

I understand, Mr. Chair, that my colleague, Larry Brock, is on the speaking list and will be next to speak. In the interests of ensuring that this committee can continue with its very important study of Bill C-26, but also continue and accelerate the study that was already agreed upon by this committee on October 23, on the motion put forward by our colleague in the Bloc Québécois, Ms. Michaud, I will cede the floor to my colleague, Mr. Brock, so that he can move the appropriate amendment.

Thank you, Mr. Chair.

● (0835)

The Chair: Mr. Brock.

Mr. Larry Brock (Brantford—Brant, CPC): Thank you, Chair.

The amendment now being proposed reads as follows: That all the words after the word “committee” in the first paragraph—

Mr. Peter Julian (New Westminster—Burnaby, NDP): Mr. Chair, I have a point of order.

The Chair: Mr. Julian.

Mr. Peter Julian: We don't have the motion. There's no motion, so you can't move an amendment if there's no motion.

Mr. Dane Lloyd: I moved the motion in my speech just now.

The Chair: Did you move the motion?

Mr. Peter Julian: He did not.

Mr. Dane Lloyd: The motion has been circulated to the committee. It was circulated on Wednesday.

Mr. Peter Julian: The motion has not been moved.

The Chair: Can you read the motion, Mr. Lloyd?

Mr. Dane Lloyd: Yes, Mr. Chair.

The Chair: Thank you.

Mr. Dane Lloyd: Mr. Chair, the original motion reads as follows:

> That the committee report to the House its acknowledgment that convening a National Summit of politicians and insiders to discuss auto theft will not prevent such theft. It also recognizes that preventing auto theft falls squarely under the federal responsibility of the Canada Border Services Agency (CBSA), the Royal Canadian Mounted Police (RCMP), Transport Canada, and Public Safety Canada.
>
> And recommend to the House that the government:
>
> A) Immediately reverse changes to Bill C-5, which allows car-stealing criminals to be on house arrest instead of serving jail time.
>
> B) Strengthen Criminal Code provisions to ensure that repeat car-stealing criminals remain in jail.
>
> C) Provide CBSA and our ports with the necessary resources to prevent stolen cars from leaving the country.

That is my motion, Mr. Chair.

Mr. Peter Julian: I have a point of order.

The Chair: Yes, Mr. Julian.

Mr. Peter Julian: Mr. Chair, I would suggest that this is out of order, for two reasons.

In terms of what the House has already considered, the House considered yesterday a substantially similar motion, and Parliament, the House of Commons, decided not to proceed with that motion. As you know, this is a very rare occurrence, Mr. Chair. Ultimately, when a bill is defeated, you can't, the next day, suggest at a committee that the bill be considered. In this case, it was an opposition motion, and it was defeated. Now the Conservatives are proposing substantially the same motion today at committee.

This is something that doesn't have precedent, Mr. Chair. It's shameless that, when Parliament decides something, members of the committee would try to come back with what is substantially the same consideration. It is true that if this was three or four years from now, you could say, "Well, things have substantially changed since Parliament considered this issue, so we should have more discussion and debate on the issue." In this case, it was yesterday; it was last night, 14 hours ago, when Parliament decided that the motion was inadequate.

I moved an amendment on behalf of the NDP, as you'll recall, Mr. Chair, talking about cracking down on organized crime, cracking down on money laundering, and restoring the cuts to the crime prevention programs that the Harper government put in place. The Conservatives rejected that, so the motion that was offered yesterday in the House was profoundly weak and contained a lot of disinformation. That's why Parliament defeated it. We can't come back the next day and consider substantially the same motion.

As you note, Mr. Chair, the intention would be to "recommend to the House". The House made the decision yesterday. The intent of the motion today is to recommend to the House the same thing. There is an issue of repetition that is, in all our procedural manuals, something that is very clearly prohibited. You can't keep bringing up the same issue in the same form.

Second, I would suggest that, because it recommends to the House, it is trying to do indirectly what is prohibited directly. In other words, it's trying to use a committee to reconsider something that was considered yesterday by the House of Commons.

The Chair: Thank you, Mr. Julian.

We're going to suspend for a couple of minutes so that I can confer with the clerk.

● (0835)

_____(Pause)_____

● (0840)

The Chair: I call the meeting back to order.

I take into consideration your comments, Mr. Julian.

After speaking with the clerk, I will say that the motion hasn't been put before the committee prior to.... I don't have the other motion in front of me right now to compare it to, so our authority is basically saying that we're going to continue with the motion and allow it to stand at this time.

Mr. Peter Julian: Mr. Chair—

Mr. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Mr. Chair, I challenge that decision, please.

The Chair: Certainly.

Mr. Peter Julian: You beat me to it, Peter.

Mr. Peter Schiefke: I'm sorry. I think this is ridiculous.

The Chair: Mr. Julian, do you want to speak after that? I gave you the opportunity there. You were both at about the same time.

Mr. Peter Julian: I hope we can vote on this.

Our witnesses have given us a tremendous amount of content, and I have tons of questions. Quite frankly, I'm a little frustrated with all the disruption that the Conservatives have caused over the last few meetings on another subject that they have then decided to drop to try to do this subject.

It's time to start questioning the witnesses.

Mr. Dane Lloyd: Is this a point of order?

The Chair: We're challenging the chair's ruling. We'll have a recorded vote.

(Ruling of the chair overturned: nays 6; yeas 5)

The Chair: The ruling of the chair has been defeated.

We move on now to—

● (0845)

Mr. Peter Julian: Mr. Chair, I move that we use this time to question the witnesses, who have given us such important testimony.

The Chair: That's the process, yes.

Mr. Bittle, you're up.

Mr. Chris Bittle (St. Catharines, Lib.): That's excellent. Thank you so much.

Thank you so much to the witnesses for being here.

It's truly disappointing to see, on issues of such importance, the Conservatives attempting to hijack this once again when they stand up and pretend to care about security.

Mr. de Boer, you mentioned mandatory reporting, not only here but with respect to the executive order in the United States. Bill C-26 requires mandatory reporting for affected sectors when there is a cybersecurity incident. Do you believe that this is important, and if so, why?

Dr. John de Boer: Through the chair, thank you for the question.

Yes, it is very important. As well as the executive order, the United States also passed a separate law in 2022 requiring it. The reason it's important is that critical infrastructure entities affect the lives of every single Canadian. We depend on it. Our economy depends on it. This is about our economic security and our national security, and requiring entities to report those incidents within a reasonable time—and I would suggest aligning it to the United States and the EU, which have 72 hours—would be an important idea. It is fundamental.

Mr. Chris Bittle: Mr. de Boer, Mr. Bradley raised some concerns about reporting. Do you share those concerns?

Dr. John de Boer: Absolutely. I share the concerns about there needing to be protection for liability, absolutely. There also needs to be a due diligence requirement. In essence, if there were good-faith attempts to report or to put in place cyber-protections to prevent cybersecurity events, that needs to be respected.

We're dealing with highly sophisticated actors. The report that came out yesterday from the U.S. government talked about a Chinese-backed actor that had been in critical infrastructure for nine months. These are highly sophisticated.

We need to act as a team. I support those amendments as well.

Mr. Chris Bittle: Thank you so much.

Ms. Quaid, what safeguards are currently in place to ensure that our critical infrastructure providers are taking action to ensure their systems are sufficient to repel cyber-attacks launched by criminal organizations and international adversaries?

Ms. Jennifer Quaid: Our critical infrastructure sectors are perhaps some of the most sophisticated. They have some of the most sophisticated cyber-defences in all of Canada and are very much aligned with the same sectors in other countries, particularly on the electricity side because of the cross-border side, as well in as finance and telcos.

What systems are in place to ensure that? They have regulators that are extraordinarily diligent—that would perhaps be a good word—in ensuring they are aligned and they have strong defences in place.

There's really nothing that we can add to what the regulators have suggested, but this regulation is important because, to further what John was saying, reporting is one of the biggest challenges we have. We don't have good numbers. We don't know how big the problem is in this country, because the reporting is different. What is defined as a cyber-incident in different reports comes across differently: who has to report, when they have to report and what is reported. We don't have reliable numbers, and that's part of the problem we have.

Mr. Chris Bittle: What risks, if any, do you see if this legislation is not passed or if we delay it too long?

● (0850)

Ms. Jennifer Quaid: There are huge risks. These are risks that start with how we will lose the faith of our Five Eyes partners. We will lose the faith and trust of the cross-border relationships that we have through NERC and FERC and all the other ones. We will also lose resources and revenue.

Mr. Chris Bittle: Thank you so much.

Do you think this legislation strikes the right balance in capturing only those firms deemed vital to national security?

Ms. Jennifer Quaid: In my remarks, I did comment on the rest of the economy.

The truth is, the rest of the economy largely supports these six sectors: the supply chain, which this legislation does cover. Critical infrastructure is now required to be aware of and responsible for the reporting of their supply chain. It does go down the chain. It's a very good start.

Mr. Chris Bittle: Thank you.

Mr. Bradley, in order for this regime to be successful, I hope you all agree that designated operators must be confident that the proprietary and commercially sensitive information they provide to the government is handled appropriately. Would you agree?

Mr. Francis Bradley: Yes.

Mr. Chris Bittle: The bill currently includes a regime aimed at protecting confidential information. What are your thoughts on this regime found within the bill?

Mr. Francis Bradley: Our concerns are more with respect to treating different entities within the Government of Canada differently when it comes to the protection and the use of information, specifically with respect to the Canadian cyber centre. That's where our area focuses with respect to the use of the information itself.

Mr. Chris Bittle: Thank you so much.

The Chair: Ms. Normandin, go ahead for six minutes, please.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): Thank you, Mr. Chair.

I also want to thank all the witnesses for their participation, which is greatly appreciated.

I'll start with Mr. Bradley.

You spoke about the risk of regulatory duplication with the North American Electric Reliability Corporation. I was wondering whether this risk of duplication comes into play at other levels. I know that you had discussions, particularly with Hydro-Québec, before you came to give your presentation. Were these types of concerns raised with regard to Quebec's privacy regulations, for example?

Is there a risk of not just duplication, but triplication in certain aspects of the regulations?

Mr. Francis Bradley: Thank you.

[*English*]

That is absolutely an excellent question.

My remarks and our brief focus specifically on that interface between the bill and our NERC requirements, which are quite onerous. The member is absolutely correct. There are other requirements that come into play at the different levels of government, as well, and also internationally. It isn't solely a matter of Bill C-26 coming into conflict with NERC. There are other levels, as well.

Our particular area of concern, where we see the potential for a significantly increased burden, is that lack of alignment between the NERC requirements, which have been in existence for many years, and what is being proposed in Bill C-26.

[*Translation*]

Ms. Christine Normandin: Thank you. This brings me to a question for Mr. de Boer.

You also spoke about alignment. I would like you to talk about the Five Eyes and the global alignment of incident reporting.

There are standards at a number of levels, and the issue becomes extremely complicated. At which level should alignment be a priority, and why?

[*English*]

Dr. John de Boer: My recommendation would be to align with the United States.

As I mentioned earlier, even the Canadian Centre for Cyber Security has mentioned that an incident affecting critical infrastructure in the United States would affect Canada. Much of our critical infrastructure—whether it be energy, rail, transport or, in some cases, telecommunications—crosses borders. We need to align with them. That would be mine: a 72-hour reporting requirement.

The other thing is aligning our definitions of what a cyber-incident is. Currently, the United States is undertaking a study through CISA to define "cyber-incident" and what is reportable. They have 52 different regimes of reporting in the United States. Imagine an entity dealing with a cybersecurity incident and being required to report to 10 or 15 different entities with different types of cyber-incidents.

If it's not aligned, this legislation will actually add to the problem, not resolve it.

● (0855)

[*Translation*]

Ms. Christine Normandin: Thank you.

Ms. Quaid, you recommended that the bill be expanded to include voluntary collaboration among companies. However, this would mean a greater need for workers to implement Bill C-26.

Was this part of your thought process? Is the widespread labour shortage a potential issue? I put this question to the committee earlier, and to the Communications Security Establishment, or CSE. I was told that this could be an issue.

I want to know whether this is an issue for you too, and if so, whether you have any possible solutions.

[*English*]

Ms. Jennifer Quaid: Thank you for the question. I'm very glad we can address the labour shortage here.

What I suggested was enabling organizations in Canada to report, speak publicly and share information about threats, attacks and incidents without fear of liability. In doing that, we're minimizing the labour impact. We're enabling companies to share information so they don't all need to have specialists doing exactly the same thing. We're enabling companies to share information so the smaller organizations with less sophisticated teams have an opportunity to learn from the larger organizations to protect themselves in advance of an attack.

What I'm hoping is that, by opening up the ability to collaborate not just with government but also broadly without fear of liability, we will, in fact, have a positive impact without adding to labour force requirements.

[*Translation*]

Ms. Christine Normandin: Thank you.

I would like to hear from anyone who wants to address the responsibility issue, even if it means a second round.

I'm concerned that, if we completely remove the responsibility of large companies, which could have a team to do the job properly, they may somehow avoid feeling the need to comply with Bill C-26.

Is there a risk of completely removing the idea of responsibility?

[*English*]

Ms. Jennifer Quaid: I think my colleague Francis Bradley talked about safe harbour legislation, which is what they call it in the U.S. It's what they have in the U.S. Through the effective drafting of something like what they have in the U.S., we can create that fine balance, and that's what we would always aim to do. You never want to remove all responsibility, but certainly remove personal liability from our CISOs, who are in very short supply, and one of the speakers last week mentioned that they're leaving at a rate of 75% right now.

We are at risk, but I think that, with effective drafting of this legislation, we can create balance so that we are not removing all liability but we are protecting organizations from liability when they are trying to share information to help others.

The Chair: Thank you, Ms. Normandin.

Mr. Julian, go ahead, please, for six minutes.

Mr. Peter Julian: Thank you very much, Mr. Chair.

Thanks to our witnesses. You've given us a lot of food for thought. I have a lot of questions. I hope that there are no further disruptions because, quite frankly, my Conservative colleagues haven't asked a single question on Bill C-26 to date, and I think that has to change. This is important legislation.

I have two questions for all three of you.

First, Ms. Quaid, you mentioned that further delays would cause loss of the faith of our partners. The government introduced this in June 2022. We're now in February 2024. We're seeing delays and disruption from the official opposition in trying to process this legislation. Beyond losing the faith of our partners, what are the other consequences? We've had previous witnesses say that, basically, Canada is increasingly becoming a target because we don't have legislation in place. What are the consequences of further delay? That is for all three of you.

My second question is based on your excellent brief, Mr. Bradley, talking about doing consultation during the regulatory process. To what extent has the industry been consulted by the government in the legislation to date? To what extent was there input so that we get this bill right?

I'll start with Mr. Bradley and then go to Mr. de Boer and Ms. Quaid.

Mr. Francis Bradley: Thank you very much. Those are two very good questions.

On the first question, with respect to the consequences of delay—and this relates to your second question as well—we've been engaged in discussions about this gap, given that we're a sector that has had mandatory reliability and mandatory critical infrastructure protection standards for a decade and a half. We have been asking the question, "What about those other sectors upon which we rely?", because the sectors are interdependent. Some sectors have robust programs and, as for others, we just don't know, frankly.

We've been in favour of seeing something broader across different critical infrastructures, those other infrastructures that we depend on. We have a very high level of confidence in the regime that we have, because it is mandatory and enforceable. We would like to see something in place, and this has been the conversation that we've been having with the government for a very long time about other sectors upon which we rely.

I think Bill C-26 does fill that gap. It overlaps—and I did talk about that in my comments—but, with respect to consultation, in terms of agencies and departments of the government, we have been talking about this for more than a decade. This is something that we've been consulted on extensively, certainly, but it is something that has been a gap for quite some time.

● (0900)

Mr. Peter Julian: Go ahead, Mr. de Boer.

Dr. John de Boer: Yes, I would echo previous comments.

Critical infrastructure is called critical infrastructure because it's essential to our daily lives and the functioning of our economy. That's critical, but there are other elements to this. If the public believes that government has not acted to protect that critical infrastructure and secure our lives, it's the very trust in our government that could be eroded.

Affordability is another potential impact. Cyber-attacks increase costs. Currently, there are countries—the U.K., notably—where insurers will refuse to provide insurance costs to actors who have been attacked by a state-sponsored actor. All those costs are passed on to consumers, so that could also be—

Mr. Peter Julian: Can I interrupt to ask you this? Do any of the three of you have figures that you could provide us with in terms of costs, increasing costs, because of the lack of action at this point?

Dr. John de Boer: I can get back to you on that in terms of certainly increasing insurance premium costs, as well as increasing costs in terms of affordability. I can get back to the committee on some of those figures.

There's a tremendous series of consequences that are fundamental to our economy. You just need to look at, for instance, Ukraine. Their electrical grid was shut down. Look at Oldsmar, Florida, where a cyber-attack almost poisoned their water system. You can go to catastrophic ends.

In terms of consultation, there has been consultation. Our frustration is that this has moved far too slowly. It needs to be considered also in conjunction with the critical infrastructure strategy, which has not been updated since 2009. What is defined as critical infrastructure needs to be aligned with the critical infrastructure entities outlined in this legislation, and that's all Public Safety's responsibility.

Mr. Peter Julian: Ms. Quaid, I'll come back to you, but you'll be cut off, unfortunately.

Ms. Jennifer Quaid: Okay. I'll keep it very short.

What are the impacts if this legislation doesn't pass? Well, look at what happened with the Colonial gas pipeline. There is at least one death confirmed to be attributed to that. What's the impact? Death. Let's be simple. If gas doesn't flow, if phone systems don't work, people will not survive.

There are also the additional impacts, as Mr. de Boer was saying, such as insurance premiums. It's increasingly difficult to get insurance. My own cyber-insurance has gone up exponentially, which means costs associated. I will have to pass that on to customers. There's the increased cost of doing business. Businesses will go down. Small and mid-size businesses cannot afford a cyber-attack. The cost of remediation is usually in the millions of dollars. Those costs have to go somewhere.

In terms of collaboration, if I can—

The Chair: Thank you, Mr. Julian and Ms. Quaid.

Mr. Peter Julian: I'll come back.

The Chair: I'm sure you'll have another opportunity.

That's round one. We're moving into round two now.

Mr. Motz, you're up for five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you very much, Chair.

Thank you to our witnesses for being here.

I know it's been stated, the rush to get this through. We've waited since June 2022, when it was put on the books, and we're still doing a little dance.

I've heard witnesses say, so far, that we need to ask ourselves what's more important, rushing this bill through even though it's faulty or trying to at least fix it so that it's workable to get some things right moving forward. That's something I'll ask all of you to respond to.

I want to also include in that response.... There has also been a concern by witnesses that the bill is vague in many areas, and the regulations are going to try to fix the gaps. The recommendation has been that there should be more definitions, that there should be other language that provides clarity in the bill rather than in the regulations, because regulations could take another couple of years to finish. That's the concern we all have.

I'd like to get your thoughts on those. I'll start with you, Ms. Quaid.

● (0905)

Ms. Jennifer Quaid: I would say that there's a balancing act. The bill is important; there is absolutely no question. There's also no question that it needs some modification. I think that with a little effort, enough of the bill can be fixed effectively to make it good legislation that can then be fine-tuned in the regulations. I think that with focus and effort, we can get it right and get it now.

Mr. Glen Motz: Mr. de Boer.

Dr. John de Boer: I fully agree. We need to get this moving now.

It's never going to be a perfect bill, but we need to make the adjustments we suggested, which are to clarify what is considered a cyber-incident and align it with the U.S.'s definition, and reporting timelines, as well. Clarity is really essential in times of crises, and so we need to do that.

Those are easy fixes. Those are things that we can probably fix with a few modifications. I would fill those gaps, get this passed and continue to work on other elements.

Mr. Glen Motz: Thank you.

Mr. Bradley.

Mr. Francis Bradley: Thank you very much.

Mr. Chair, this is an excellent question. Do we rush the bill through or do we amend it to make it right? My response is, let's do both. Let's rush this bill through, but rush it through while taking into consideration the 14 recommendations that we've made and make the amendments that respond to those 14 recommendations.

Mr. Glen Motz: Thank you.

I'm going to stay with you, Mr. Bradley.

You indicated in your written brief that the bill risks "adding very little security to our sector". I was a bit troubled to read that. Certainly our electrical grid and the reliability of electricity are some of our most critical infrastructure components. You then state further that the bill "should provide tools and protocols to add to the safety of Canada's infrastructure sector." What are those specific protocols and tools that you mentioned, if you haven't already mentioned them in your opening?

Mr. Francis Bradley: Thank you very much.

With respect to the bill not significantly adding to the security, and in fact potentially diverting attention, it is not an issue with the bill itself. It's that the bar has already been raised higher than what's in Bill C-26 as a result of the mandatory standards our sector is already subject to through the North American Electric Reliability Corporation standards regime. That bar has already been set higher.

What has been put in Bill C-26 does not improve upon that. It detracts. It diverts attention to a separate and second parallel reporting structure, as opposed to using those resources to work on a response.

Mr. Glen Motz: All right. Thank you.

Mr. de Boer, the Canadian Chamber of Commerce has indicated that a patchwork is a disadvantage to business if we don't get this right. BlackBerry produced a white paper back in 2022. The biggest obstacle you saw, which was mentioned briefly already, was the lack of skilled people and skilled resources to deal with this at the critical infrastructure business level first, and then maybe in a larger threat environment.

Do you see that changing since 2022, when that was written?

Dr. John de Boer: I also co-chair, with the Canadian Chamber, their "Cyber. Right. Now." council, so—

The Chair: I'm sorry to interrupt, but I have to make this a hard stop. We're running out of time, and I want to make sure everybody has an opportunity.

Mr. Gaheer, go ahead, please.

● (0910)

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair.

Thank you to all of the witnesses for making time for this committee.

My questions are largely for Mr. Bradley from Electricity Canada.

How many organizations are represented under your organization?

Mr. Francis Bradley: Forty companies are principal members of the association, from the largest electricity companies in the country, such as Hydro-Québec, down to the municipal utilities in Ontario.

Mr. Iqwinder Gaheer: How many of those organizations currently have a cybersecurity program in place?

Mr. Francis Bradley: All of them.

Mr. Iqwinder Gaheer: I would assume that there's a little bit of variability in the different programs at different organizations.

Mr. Francis Bradley: Absolutely. Depending on the size of the organization, of course there would be variability, but all of those that are involved in the bulk power system are covered by the North American Electric Reliability Corporation's mandatory cybersecurity standards. As a result, those companies have very robust and consistent cybersecurity programs.

Mr. Iqwinder Gaheer: Okay.

What are the consequences of a successful cyber-attack against a critical infrastructure operator in the energy sector?

Mr. Francis Bradley: As has been mentioned already by this panel...not in Canada but in other jurisdictions. We've seen a loss of pipeline in the United States. In Ukraine, in 2015, we saw, for the first time anywhere in the world, a successful cyber-attack resulting in a loss of power to customers. That's not something that's happened here, but those are the potential consequences of cyber-attacks.

Mr. Iqwinder Gaheer: Obviously, this is a very vital sector. I think everyone here understands that. I think that's why I was a little bit surprised when you spoke in your opening testimony against the mandatory requirements in this bill and spoke against the immediate reporting.

When I listened to the testimony by Ms. Quaid, she indicated that reporting varies and the data is not reliable. I just wanted to get your take on that.

Mr. Francis Bradley: When a cyber-event is occurring, do we want our people working on paperwork for regulators or do we want them, at that moment, working on securing the systems? First and foremost, we want to have people working on securing the systems, and then looking at the reporting requirements.

It's a question of easing the reporting and regulatory burden, number one. Number two, my concern is about duplication here. We already have reporting requirements. We're talking about now creating a second reporting regime as well.

Mr. Iqwinder Gaheer: You mentioned that this other regime is actually a higher standard. Wouldn't it be easier to meet the lower standard contained within this bill?

Mr. Francis Bradley: It would be, except that if the definitions are going to be different, it means having a separate and different reporting structure and different definitions.

In fact, not entirely joking, I said a number of years ago, when the government was beginning to move along this path, that they potentially could look at the NERC cybersecurity standards and look at replicating those for other Canadian critical infrastructure sectors. That would have made our life easier, certainly, if we'd looked at the existing regime we had and looked at applying it to other sectors.

Mr. Iqwinder Gaheer: I guess you would agree that, whether it's this regime or another regime, mandatory reporting requirements are important and information collection is important.

Mr. Francis Bradley: Absolutely.

Mr. Iqwinder Gaheer: Thank you, Chair.

The Chair: Ms. Normandin, you have two and a half minutes, please.

[*Translation*]

Ms. Christine Normandin: Thank you, Mr. Chair.

My question is for all the witnesses. They should feel free to answer it.

Bill C-26 strikes a type of balance between the items already enshrined in the bill and the regulations. I gather that many definitions will come from the regulations, penalties, all the people involved, and so on.

Cybernetics is a fast-paced sector. While regulating a good portion of the sector can provide some flexibility, it can also hamper efforts to keep smaller companies up to date and informed of the latest developments.

I would like you to comment on the balance between the two.

[*English*]

Dr. John de Boer: I think there still needs to be clarity in terms of some of the definition issues. For equilibrium in terms of, for instance, sanctioning and fines, etc., there needs to be some level of consequence for negligence—for failure to implement a baseline cybersecurity standard.

There also needs to be encouragement for large critical infrastructure entities to ensure that their supply chain is secure. That means working closely with the small and medium-sized businesses.

The other thing I would add is that in the United States, the U.S. government has created a grant program to enable critical infrastructure entities to put in place certain baseline cybersecurity requirements. That could be another suggestion.

The last thing I would mention in terms of the right equilibrium is that this law pushes a prevention-first approach. We know that in medicine, prevention is oftentimes better than the cure. Let's get people to invest up front.

● (0915)

Ms. Jennifer Quaid: If I can pick up on what Mr. de Boer was saying in terms of incentives for those small and medium organizations, if we enable the larger organizations to share openly, truthfully and fully with the small and medium organizations about what they're seeing and doing, and support them so that they don't get hit with the same attack, the prevention is better than the cure. That will help.

Another approach we could take is to incentivize businesses that are not necessarily the ones covered by this legislation—that's a separate piece—but the supply chain. We can incentivize the supply chain to reach a level of cyber-maturity through tax incentives or through insurance breaks, if they have certifications.

The Chair: Thank you, Ms. Normandin.

For our last questions, we'll have Mr. Julian, please.

Mr. Peter Julian: Thank you, Mr. Chair.

I'd like to congratulate Mr. Motz on asking the first question for the Conservatives on Bill C-26, a month into the study.

I'd like to go back to you, Ms. Quaid, on the issue of consultation.

There's also the question of whether or not we're increasingly a target because of the lack of action and delay around important legislation.

My third question comes back to your recommendation around expenses for joining, if I have this correctly, the Canadian Cyber Threat Exchange. To what extent would that be a cost? You said there is no cost, but I'm sure there would be. Have you evaluated what that would be and what the advantages are from that?

Those are three questions for two minutes.

Ms. Jennifer Quaid: I'll take the last question first, which is the reference to joining the CCTX.

In fact, I said a Canadian cyber-collaboration organization—not necessarily ours, although that would be wonderful. When I said there's no cost, it's that there's no cost to the government for that because it would be part of the ITB program. Any of the organizations or companies that are working through or impacted by the ITB program could join a threat-sharing association, so that they can be more aware of what's going on in the cyber-ecosystem, such as what the attack vectors are likely to be, and remediation and resiliency solutions.

That's the first one. There's no cost to the government. There is a cost for us, but it's nominal for small businesses. It's really small.

I believe the other question you had earlier was on consultation.

Mr. Peter Julian: It was on the consultation process.

Ms. Jennifer Quaid: There was certainly an opportunity for consultation several years ago. We participated in that with our members, as well, because we reached out to them. It became a trickle-down process, but it would be nice to see something like Bill C-26 running in concert with a national cyber-strategy.

The consultation was several years ago and is now two years behind. I see that coming down the pipeline.

What was the third question?

Mr. Peter Julian: The third question was whether it is true, as some witnesses have pointed out, that Canada is increasingly a target because we haven't put in place cybersecurity measures.

Ms. Jennifer Quaid: That may be harsh. Canada is increasingly a target because it pays ransom. There are countries that organizations intentionally don't attack because they don't pay ransom. Canada generally pays ransom—

The Chair: Thank you, Ms. Quaid.

Mr. Julian, that's your time.

Thank you so much to the witnesses for being here today on a very important topic.

We're going to suspend—

Mr. Glen Motz: Chair, can I just ask the witnesses a question?

If there's anything further that came up today from the questions being asked that you couldn't give a fulsome answer to, could you please provide it to the committee for our deliberations and report?

Thank you.

The Chair: Thank you.

We're going to suspend for five minutes and get ready for another round of witnesses.

Thank you so much for being here.

● (0915)

(Pause)

● (0925)

The Chair: I would like to welcome our second panel of witnesses.

By video conference, from Canada Energy Regulator, we have Chris Loewen, executive vice-president, regulatory; and Christopher Finley, director, emergency management and security.

In person, we have, from the Canadian Radio-television and Telecommunications Commission, Steven Harroun, chief compliance and enforcement officer; Anthony McIntyre, general counsel and deputy executive director, legal services; and Leila Wright, executive director, telecommunications.

We'll be giving up to five minutes for opening remarks, after which we will proceed with rounds of questions. Welcome to all of you.

I now invite Mr. Loewen to make an opening statement, please.

Mr. Chris Loewen (Executive Vice-President, Regulatory, Canada Energy Regulator): Good morning.

My name is Chris Loewen. I am the executive vice-president, regulatory, at the Canada Energy Regulator. I'm joined today by Mr. Chris Finley, director of emergency management and security.

Thank you for inviting the Canada Energy Regulator to appear before the committee today to discuss Bill C-26.

We join you today from Calgary. I would like to take this opportunity to acknowledge the traditional territories of the people of the Treaty 7 region of southern Alberta.

[*Translation*]

I'll start by outlining the mandate of the Canada Energy Regulator, or CER.

The CER regulates infrastructure to ensure the safe and efficient delivery of energy to Canadians and the world. It regulates pipelines, power lines, energy resource development and energy trade on behalf of Canadians in a way that protects the public and the environment while supporting efficient markets.

[*English*]

Safety is at the core of our work. We regulate to prevent harm in all forms, and we understand that this includes the cybersecurity threats that Bill C-26 is seeking to address. The CER takes the matter of cybersecurity threats to Canada's energy supply seriously.

The CER oversees roughly 71,000 kilometres of the oil and gas pipelines in Canada. We regulate pipelines that cross provincial boundaries or the Canada-U.S. border. CER-regulated pipeline companies are required to have proactive measures in place to protect this critical infrastructure from cybersecurity threats.

Regulated companies must have a security management program that anticipates, prevents, manages and mitigates conditions that could adversely affect people, property or the environment. In addition to the physical threats to infrastructure, companies must consider cybersecurity threats in their security management program and implement appropriate mitigation based on the results of a security risk assessment process. These requirements are laid out in the Canadian Standards Association's Z246.1 standard, which is included in the CER Act's onshore pipeline regulations by reference.

Cybersecurity measures must reflect the criticality of cyber-assets, as well as the results of regular assessments of threats, vulnerabilities and overall security risk.

The regulation of electricity generation, transmission and distribution rests primarily within the jurisdiction of provinces and territories. However, the CER regulates approximately 1,500 kilometres of international power lines. The Canadian public rightfully expects us to hold the pipeline and international powerline companies we regulate accountable for the safe operation of CER-regulated energy infrastructure.

The CER is well positioned to administer the obligations of Bill C-26, in particular those that apply to companies we regulate, and, given these obligations, align with those already found in the Canadian Energy Regulator Act.

For example, the bill provides the CER with the ability to issue orders and to take necessary enforcement actions to bring a company back into compliance, so that critical cyber systems are protected.

● (0930)

[*Translation*]

The CER already uses similar tools. For example, it issues notices of non-compliance, inspection officer orders and administrative monetary penalties, as needed, to bring companies back into compliance and ensure that they operate safely.

The CER also verifies that companies are meeting requirements through inspections, audits, compliance meetings and emergency response exercises.

[*English*]

The CER uses an integrated government approach. It works with federal, territorial, provincial and international agencies, as well as regulated industry, to ensure that proactive measures are taken to protect federally regulated energy infrastructure from cyber-related risks or attacks.

Thank you very much for the opportunity to speak with you today about this important issue. We look forward to your questions.

The Chair: Thank you, Mr. Loewen.

Ms. Wright, go ahead.

Ms. Leila Wright (Executive Director, Telecommunications, Canadian Radio-television and Telecommunications Commission): Good morning, and thank you for inviting us to speak with you this morning.

Before I begin my remarks, I would like to acknowledge that we are gathered on the traditional unceded territory of the Anishinabe people.

My name is Leila Wright, and I am the executive director of telecommunications at the CRTC. I am joined today by my colleagues Steven Harroun, chief compliance and enforcement officer, and Anthony McIntyre, general counsel.

[*Translation*]

The CRTC is an independent and quasi-judicial tribunal that operates at arm's length from the government. We hold public hearings on telecommunications and broadcasting matters. We make decisions based on the public record.

[*English*]

In the telecommunications industry, our work focuses on increasing competition for Internet and cellphone services. We do this by promoting greater choice and affordability for Canadians, encouraging investment in reliable and high-quality networks, and improving access to telecommunications services in indigenous, rural and remote communities. We also have a team that helps protect Canadians from unwanted emails, texts and online scams.

[*Translation*]

The CRTC plays a small part in the federal government's effort to protect the security of Canada's telecommunications system.

[*English*]

Other organizations that contribute to this effort include the Communications Security Establishment, the Canadian Security Intelligence Service, Innovation, Science and Economic Development Canada, the Canadian security telecommunications advisory committee and many others.

The CRTC does not have a role to play within the proposed critical cyber systems protection act. Additionally, many of the proposed amendments to the Telecommunications Act establish new authorities exclusively for the Governor in Council and the Minister of Industry, and do not modify the CRTC's regulatory mandate under the act.

● (0935)

[*Translation*]

However, a few changes would be relevant to the CRTC's work. I'll focus on three changes in particular.

[*English*]

First, the proposed amendment to section 7 of the Telecommunications Act would add a new policy objective focused on promoting the security of the Canadian telecommunications systems. As with other policy objectives set out in the act, this addition would allow the CRTC to expressly consider how its decisions could further this new objective.

Second, the addition of proposed section 15.6 would facilitate information sharing between a broad group of security-focused government departments and agencies and the CRTC. This would be for the purpose of ensuring compliance with orders and regulations made by the Governor in Council and the minister.

[*Translation*]

Third, section 47 would require the CRTC to take into account any orders or regulations made by the Governor in Council and the minister in its decision-making.

[*English*]

Should Parliament adopt Bill C-26, the CRTC will be ready to implement the amendments made to the Telecommunications Act that affect our work.

Thank you again for inviting us to speak today. We look forward to your questions.

The Chair: Thank you, Ms. Wright.

We're going to move right on to the questions.

Mr. Shipley is up first, for six minutes.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair.

Thank you to all the witnesses for being here today.

In the first hour of witness testimony this morning, we heard a shocking number from Mr. de Boer, who said that 5.2 million cyber-attacks were stopped. That number shocks me.

I'd like to know, through Mr. Loewen, as the regulatory board for your energy sector, how many of those you are seeing in the area that you're responsible for.

Mr. Chris Loewen: Thank you very much for the question.

I would have to say that it's one of the reasons why reporting is going to be very important with respect to the proposed legislation. We currently rely on reporting from companies that provides us with an understanding of the magnitude but not the actual specific number of cyber-threats or cyber-attacks that are occurring with respect to our companies. Regulated industry is targeted by a number of threats from domestic and state actors. I would say that they vary from password theft and document theft all the way up to ransomware and other types of malware.

I might just turn to my colleague, Mr. Chris Finley. He might be able to provide you with a better sense of the volume.

Mr. Christopher Finley (Director, Emergency Management and Security, Canada Energy Regulator): Thank you for the question.

To date, the Canada Energy Regulator has no evidence of any cybersecurity incidents suffered by regulated companies that have affected the operation of a pipeline—in other words, their operational technology network. Admittedly, we also have had no reported incidents that have caused a cybersecurity event. There is a series of reportable incidents in our regulations. There has been nothing reported to date.

In terms of our regulated industries, of course, they are always under threat. Many of those attacks are below the bar, and we certainly wouldn't hear about those. As well, there is voluntary reporting currently to the Canadian cyber centre.

Mr. Doug Shipley: Thank you.

I think that somewhere in there there was a little bit of good news for us. As I said, with that number of 5.2 million at the beginning, hearing yours at considerably less than that obviously will help us sleep a little better at night.

How will Bill C-26 change the way you do business overall? Will it help your members and help you? What's the main implication, if and when this is passed, for how it's going to change?

● (0940)

Mr. Chris Loewen: The proposed legislation is well aligned with the CER's oversight mandate. We already have a fairly robust regulatory framework in place that requires companies to identify and anticipate threats and risks to their systems, processes and operations and to have programs in place that prevent and mitigate those events. We also have in place inspection officers with the ability to issue non-compliance inspection officer orders and, where necessary, administrative monetary penalties.

You can see that the elements of the proposed legislation closely mirror what we currently have in place. In addition to that, it enhances reporting and information sharing, which I think can only lead to a much stronger oversight of cyber-threats within our industry.

Mr. Doug Shipley: Thank you for that.

I'll turn to our witnesses from the CRTC this morning, probably Ms. Wright, who started off.

There have been concerns that in incidents of an order in council or a ministerial order or a regulation overriding a decision from the CRTC, there may not be a public notice or notice of decision. Do you agree that this process should be more transparent?

Ms. Leila Wright: The CRTC's role is to implement the legislation that is adopted by Parliament. Our role is not to comment on proposed legislation that is before Parliament, so unfortunately I'm not able to respond to your question.

Mr. Doug Shipley: Thank you.

Would you support provisions that require the government to table an annual report that would include the number of times government orders or regulations have prevailed over CRTC decisions?

Ms. Leila Wright: I would respectfully say that this would be a question for ISED.

Mr. Doug Shipley: I'm sorry. I couldn't hear you.

Ms. Leila Wright: That would be a question that should be posed to our colleagues at ISED.

Mr. Doug Shipley: Okay.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Shipley.

We're moving on to Mr. Schiefke, please, for six minutes.

Mr. Peter Schiefke: Thank you very much, Mr. Chair.

I'd like to thank our witnesses for being here in person and virtually.

I'll begin my line of questioning with Mr. Loewen.

Mr. Loewen, in layman's terms, for Canadians who are interested in and affected by this topic, what would be the consequences of a successful cyber-attack against a critical infrastructure operator in the energy sector?

Mr. Chris Loewen: Thank you for that question.

The consequences could potentially vary greatly and depend on the nature of the attack, obviously.

In the cyber centre's assessment, the main threat to Canada's energy sector is from financially motivated cybercriminals primarily using things like ransomware, as I noted earlier. Those attacks most typically affect information technology networks, although it is possible for them to target operational technology. The ransomware on an IT network will cost a regulated company money in potentially paying the ransom, but certainly in lost time and in recovering their infrastructure.

Ransomware on an old T-network or operational technology network such as a SCADA system, while rare, could be far more disruptive to pipeline operations. Although this would be unlikely to create unsafe operating conditions, as my colleague noted earlier, we have no evidence. We haven't heard reports of any such breach of an operational technology system in a CER-regulated industry.

Mr. Peter Schiefke: I'll follow up on that.

Given the interconnectedness of the energy sector in Canada and that of our largest trading partner and ally, the United States, how important is it, in Bill C-26, for Canada to strengthen our cybersecurity protection?

Mr. Chris Loewen: I would respond by saying that the energy sector is targeted by nation-state cyber-espionage activities that don't recognize borders. These are primarily a threat to intellectual property, such as research and business plans. Because the energy sector is a strategically important critical infrastructure and is transborder, as you noted, it is also a likely target for adversarial nation-states to sabotage, if possible, operational technology.

The impact on that would be significant.

● (0945)

Mr. Peter Schiefke: One of the main focuses in this committee is on improving the bill and looking for things that are not included in it but that we could include to strengthen it.

Is there anything our trading partner and ally, the United States, is doing that we are not doing and that is not included in Bill C-26 but that you believe should be included?

Mr. Chris Loewen: You know, we're not the lead on this particular legislation, but we did provide advice. In my view, it's very well aligned already with what we have in place at the CER.

I might turn it over to my colleague Mr. Chris Finley, as he is more familiar with some of the activities that are taking place in the United States.

Mr. Peter Schiefke: Mr. Finley.

Mr. Christopher Finley: Thank you.

We work closely with the Transportation Security Administration and the PHMSA—the Pipeline and Hazardous Materials Safety Administration. Primarily, within Canada, we work very closely with the Communications Security Establishment and their cyber centre to make sure we're in alignment internally.

We believe, as my colleague said, that the robustness of our regulatory environment, currently, is solid. However, we see a real benefit in the mandatory reporting requirements as set out in proposed sections 17, 18 and 19. We can take that information and implement it across our pipeline network to make it safer.

Mr. Peter Schiefke: Thank you, both.

I'll now turn my questioning to Ms. Wright.

Ms. Wright, thank you for being here.

A priority for all of us here, regardless of political party, is protecting the privacy of Canadians. Some witnesses have warned that this bill may result in the government accessing, collecting and misusing personal information, including personal cellphone information. In your reading of this bill, and based on your experience and position, do you see that happening?

Ms. Leila Wright: Again, unfortunately, I'm not able to respond to that question.

Our role is to implement the provisions that touch upon the CRTC's work. I've outlined those provisions. They're quite narrow, so I'm not able to respond to that question.

Mr. Peter Schiefke: Would you be able to comment on how Bill C-26 will intersect with the Privacy Act? Is there anything in the bill that affects the applicability of the act?

Ms. Leila Wright: Unfortunately, I'm not able to respond to that question.

Mr. Peter Schiefke: Okay.

I guess I'll ask you one last question before my time is up.

Is there anything that is not in Bill C-26, Ms. Wright, that you would like to see that could provide greater support for the work you're doing?

Ms. Leila Wright: Again, our role is to implement legislation adopted by Parliament, rather than comment on proposed legislation before the committee.

Mr. Peter Schiefke: Okay. Thank you, Ms. Wright.

That's all, Mr. Chair. Thank you.

The Chair: Mr. Julian, you have six minutes, please.

[*Translation*]

Mr. Peter Julian: Mr. Chair, I'll ask a question on behalf of Mrs. Normandin. I would appreciate some flexibility with my speaking time. If you don't mind, I'll ask her question first and then move on to my own questions.

Ms. Wright, my question concerns the recommendation that the committee received from Citizen Lab, which suggested that we provide relief for smaller telecommunications providers.

Should Bill C-26's regulatory framework be implemented in a manner that takes into account its impact on smaller telecommunications providers? Should the implementation of this regulatory framework be flexible enough to ensure that smaller companies can easily comply with the components of the bill?

[*English*]

Ms. Leila Wright: Thank you for the question, and I apologize if my response is frustrating to the committee.

Our role is to implement legislation that is adopted by Parliament. When it comes to the proposed legislation before the committee today, we can speak to the proposed amendments to the Telecommunications Act that touch on the CRTC's work, and also speak to how similar provisions are currently applied by the CRTC. However, I am not able to respond to your question.

Mr. Peter Julian: Okay, thank you.

I'd like to go to Mr. Loewen and Mr. Finley.

Mr. Finley, when asked by Mr. Shipley about the number of incidents, you said that nothing has been reported to date, but there may have been incidents reported to the cyber centre.

Can you explain to us, number one, whether you'd be aware of incidents that were reported to the cyber centre? Is that part of the situational report that you receive? I find it a bit surprising, quite frankly, that there's nothing reported to date. I'm assuming that means it's above a certain threshold of incidents. If you could clarify your remarks on that, that would be helpful, because, as Mr. Shipley mentioned, BlackBerry just testified to over five million attempted cyber-attacks in the last 90 days that it has been able to head off. It seems to me that the energy sector would be a target of these bad players.

● (0950)

Mr. Christopher Finley: Yes, certainly, I can clarify my remarks.

The energy sector is a target; there's no question. In answering the question, generally, there is no reporting requirement on cybersecurity incidents currently to the Canada Energy Regulator. What we do is work closely with regulated companies and the cyber centre, and we encourage voluntary reporting between our company and the cyber centre, and they create non-disclosure agreements.

They collect information, and they will share that information out to industries in a form that is not disclosing details of what those incidents were. That's, I guess, what this bill would do. It would strengthen that mandatory reporting and allow us to get access to that information more freely than now.

Mr. Peter Julian: Currently, you have no access to that information. Would it be fair to say that currently there is no sharing of best practices? If there is an attempt on an energy company, the information on how to stop that attack wouldn't be available to other companies in the energy sector.

Would that be an accurate depiction of how the situation is today?

Mr. Christopher Finley: I think the way the situation is now, in terms of reporting to the CER, there is no mandatory cybersecurity reporting, unless it meets a definition in the onshore pipeline regulations for another type of incident, such as operation beyond design, or something more significant.

That information is reported voluntarily to the cyber centre, and again, they produce reports. It may be a question for the cyber centre. They do produce threat risk reports and they distribute them within our industry and more broadly, so that certainly companies do have information or access to it to take measures to put the right mitigation in place.

Mr. Peter Julian: Okay. I appreciate your honesty on this. It's disturbing to me. Would that not mean, for example, that on the shutdown of the Colonial gas pipeline, which has been referenced by other witnesses, the information about how to stop that type of attack would not necessarily be available to Canadian energy companies and to the energy regulator? Or is it that we're getting information about attacks outside of Canada, but within Canada attacks are not necessarily shared in any way to ensure that energy companies, in this case, are able to bulwark themselves against a repetition of that attack?

Mr. Christopher Finley: I certainly think that, through the bill, it could be more structured and more formalized. Then those mechanisms would be in place to share that information officially. As you can appreciate, some of this information comes with some cautions in terms of how widely it can be shared due to confidentiality.

Again, we do have relationships, informally, with the cyber centre and with other federal departments and agencies to get that information. Through our compliance verification activities, we do look at companies' programs and systems to make sure that they are doing everything they can, that they are connected with the cyber centre and getting the latest threat and risk briefings, and that they are taking the measures they can take.

● (0955)

Mr. Peter Julian: The chair's been very generous. I just have one further question, specifically on Colonial gas.

Were you given access to the information about that attack and how to prevent an attack of that nature in the future?

Mr. Christopher Finley: That's a pipeline that was in the United States, so non-officially but certainly through various working relationships that we have with our staff in different departments, we've learned about that incident. However, I'm not prepared to comment on the details of that.

The Chair: Thank you, Mr. Finley.

Thank you, Mr. Julian.

We're moving into the second round. We have pretty good timing here.

Mr. Lloyd, you're up for five minutes.

Mr. Dane Lloyd: Thank you, Mr. Chair.

Thank you to the witnesses for coming.

My questions are going to focus on the Canada Energy Regulator.

I think there's been a little bit of confusion with this bill. Some people who are watching this might believe that if we don't pass this bill or if it gets delayed, companies won't be spending on cybersecurity. However, it's pretty clear that companies are spending a lot on cybersecurity. For example, a major integrated oil company, Cenovus, has announced in its 2024 budget that it's spending over $100 million on cybersecurity. It certainly seems that many companies across many sectors are taking this issue very seriously.

However, we just had witnesses in the last panel—I believe from Electricity Canada—who were concerned about this bill because they believe that it might not necessarily lead to a massive increase in spending on incident reporting and incident prevention but will massively increase the amount of money that companies have to spend just to comply with the legislation.

I'm wondering if you can comment. Do you foresee, under this legislation, the compliance costs for companies increasing significantly?

Mr. Chris Loewen: As I mentioned in the opening remarks, the proposed legislation is very well aligned with what we already have in place. At the CER, we already have a robust regulatory framework that involves inspection officers, inspection officer orders, the issuing of non-compliances, the use of administrative monetary penalties, and the conduct of inspections. Companies are already well familiar with the need to have cybersecurity programs in place in order to detect and prevent the threats.

In terms of the overall impact on the CER-regulated industry in terms of cost, I think that some of that detail needs to be determined through the development of regulations, which have not yet been developed or proposed. With regard to the other part of it, I would point to the fact that what the bill is proposing is, in large part, a formalization of the powers and the oversight framework that we have in place, but extending it further so that it formalizes, as Mr. Finley noted earlier, the reporting relationships, the information gathering and the sharing of that on the government side.

Mr. Dane Lloyd: If I'm clear from what you're saying, at least for CER-regulated industries, many of the practices for cybersecurity that are in this bill are already in practice. Just to summarize what you said, this bill is really just formalizing something that already exists. I think it wouldn't be a stretch to say that across a number of other sectors, including the CRTC, these practices, and in some cases regulations, already exist to ensure cybersecurity.

I'm concerned that the government is looking at formalizing this and also increasing its powers, when Canadians should be somewhat assured that, at least in your industry, there already is significant spending by the private sector on this.

Electricity Canada also said that there was a concern that this new, formalized legislation could create a chilling effect. Rather than having a very good relationship between, for example, yourself and the designated operators underneath you, where you have a very open dialogue about cybersecurity and what needs to be done, there could be a chilling effect where lawyers are advising companies to give the government only the information that's necessary under the act.

Can you comment on that chilling effect? Do you agree with Electricity Canada that there's a bit of a threat that this chilling effect could occur?

● (1000)

Mr. Chris Loewen: Thanks again for the follow-up.

To clarify, what we see already with respect to our relationships with industry is a patchwork of voluntary interrelationships with respect to reporting, usage and gathering of information.

When I use the word “formalize”, I'm saying that this is a beneficial aspect of this bill. I think industry is well prepared to implement the aspects of the bill associated with that. It will strengthen our ability as a government to prevent cyber-threats and assist our regulated industry to detect and mitigate any potential cyber-threats in the future.

With respect to the comments of Electricity Canada and the chilling effect, our experience with respect to the pipeline industry and threats to the environment, safety and other areas has been that clarity around reporting—which I expect would be something that will be developed in the regulations—not so much sets a floor, but helps with the expectations around that.

The Chair: Thank you, Mr. Loewen. Your time is up.

Mr. McKinnon, go ahead, please.

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Thank you, Chair.

My questions are for the energy regulator.

You mentioned reporting requirements and so forth, and good data. This intersects with information we heard from previous witnesses around the need for consistent and concise definitions, so that the data can be captured across the different industries and in different situations and have meaning.

Would you have comments on that?

Mr. Chris Loewen: I think that any time you can bring consistency and clarity to a sector, it's a benefit and it's a benefit for everyone.

At the CER, we have a long history of implementing our regulatory framework with respect to the onshore pipeline regulations and other regulations. The usage of things to help with the clarity around reporting requirements, such as event reporting guidelines and other directives and guidance materials, is welcomed by industry and helps them understand the expectations of the regulator. I think that, overall, it strengthens the protections in an industry. I do see that as an aspect of the particular requirements in this bill.

The regulations, as I noted earlier, are still to be developed. Should the bill pass, I'm looking forward to working with the lead departments and agencies on this bill to provide advice.

Mr. Ron McKinnon: Do you feel that these definitions are best dealt with in regulation, or should they be incorporated into the bill itself?

Mr. Chris Loewen: Not being the lead on the development of this, I would prefer to say that regulations are an area that provides some flexibility in terms of development going forward and any amendments that might be required in the future, rather than having to amend legislation.

Mr. Ron McKinnon: There was also discussion earlier about the United States undertaking an effort to provide a consistent set of definitions across their various 52-some regimes.

Is that something that would benefit us? Is it something that we are, perhaps, participating in, in any way?

Mr. Chris Loewen: I don't know if I can speak to the specific situation that you're describing, but what I would suggest is that the coordination and co-operation that we have with our counterparts in the United States, such as the Pipeline and Hazardous Materials Safety Administration, which regulates pipelines, have been very good.

Consistency of definitions is definitely something that is welcomed by industry. Consistency and a coherent regulatory framework are, I would say, a welcome development when a network can be put in place.

● (1005)

Mr. Ron McKinnon: When we talk about cyber-incidents, it seems very generic, very abstract. I wonder if you can give us some clarity on the kinds of incidents we're dealing with. What sorts of attacks are we looking at? Who are the bad actors here? Is it some hacker in his mom's basement or is it international? Could you give us some insight on that?

Mr. Chris Loewen: I'll say a few words, and then I'll turn it over to my colleague, Mr. Finley, to colour that in a little bit.

It ranges. It goes from the person in the basement to a nation-state actor.

I think earlier, when we were discussing incidents and reporting, one of the distinctions that the CER drew was the difference between an attack on an information technology network—that is the network that provides your email and stores your documents and passwords—and then the operational technology network, which is the systems that are used to operate pipeline valves and other systems. To date, there has been no successful attack that we're aware of in Canada in the CER's regulated industry on an operational network. Within your information technology networks—the ones with passwords, etc.—yes, those have happened quite frequently.

Mr. Finley, did you want to colour that in a little bit?

Mr. Christopher Finley: Yes, as my colleague mentioned, the majority of attacks are on IT networks; they're ransomware, typically by cybercriminals and nation-states. We don't have all of that information at our fingertips, but that is the kind of information that we work closely on with the Canadian Centre for Cyber Security, which does collect that information.

The Chair: Thank you, Mr. Finley.

Mr. McKinnon, thank you so much.

We'll go to Mr. Julian, please, for two and a half minutes.

Mr. Peter Julian: Thanks very much, Mr. Chair.

Ms. Wright, at the CRTC, do you track in any way incidents of cybersecurity breaches among telecommunications companies and other companies that are under your jurisdiction?

Ms. Leila Wright: The CRTC does not have a role with respect to cybersecurity.

Perhaps I will give the question to my colleague, Steven Harroun, who can speak about some of the enforcement work that we do in the space.

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): To your specific question, the answer is no. I think the Canadian Centre for Cyber Security is your best witness on that information, as my energy regulator colleague mentioned.

Mr. Peter Julian: You are not told by any of the companies that are under your jurisdiction, any of the entities, that there's been a cybersecurity breach. You are unaware of that.

Ms. Leila Wright: We work very closely with our colleagues at ISED to regulate in this space, and we can undertake to get back to you with a response.

Mr. Peter Julian: I think that would be helpful, because we've been stunned by some of the massive figures of cybersecurity breaches or attempts. This morning, we heard from BlackBerry that there were over five million in the last 90 days. Similar to the energy sector, the telecommunications sector is a vital sector and it would seem to me self-evident that there would be attacks and attempts. What I hear is that, at this point, there's no gathering of that information, and I think that's of some concern. If you have any information at all that you can provide to the committee, that would be helpful.

Can I ask to what extent the CRTC was consulted on this bill prior to its being tabled? Was there any consultation at all? Did the government reach out to you, given your regulatory role?

Ms. Leila Wright: Perhaps I can direct that question to my colleague Mr. McIntyre.

Mr. Anthony McIntyre (General Counsel and Deputy Executive Director, Legal Services, Canadian Radio-television and Telecommunications Commission): We were consulted prior to the tabling of the bill. Given the fact that our role under the amendments is very limited, we were only consulted on the few provisions that would apply to us, so we weren't involved in the policy discussion beyond what applies to us in the legislation.

● (1010)

Mr. Peter Julian: Is what you see in the legislation reflective of the feedback that the CRTC provided?

Mr. Anthony McIntyre: I don't know that I'm in a position to comment on that.

The Chair: Thank you, Mr. McIntyre and Mr. Julian.

What we're going to do is give two and a half minutes each for the final two questions.

Go ahead, Mr. Motz, please, for two and a half minutes.

Mr. Glen Motz: Thank you very much, Chair.

I'll focus my questions on the CRTC. Last year, the Auditor General reported that the CRTC was not doing enough to track the affordability of Internet and cellular services, particularly in rural and remote areas. Has the CRTC undertaken any sort of analysis of the impacts of Bill C-26 as written on the prices that Canadians pay for Internet and cellular services?

Ms. Leila Wright: Not to my knowledge.

Mr. Glen Motz: So you don't know. Okay, that's interesting.

Do you think that it will have an impact on the prices of Internet and cellular services?

Ms. Leila Wright: It's difficult for me to respond to that question without additional data and information. What I can say is that the CRTC is working very hard to promote choice and affordability for Canadians across the country, including in indigenous, rural and remote communities.

Mr. Glen Motz: I would encourage you to consider the question to see whether there is an impact.

We also know that Bill C-11 and Bill C-18 gave sweeping new powers to the CRTC. We've heard from witnesses that Bill C-26 as written also grants too much power, mainly ministerial power. How do you recommend amending the act to give Canadians the confidence that there will be proper oversight without overreach and that transparency and accountability will be balanced?

Ms. Leila Wright: I'm unfortunately not in a position to comment on the legislation that is before the committee. Our role is to implement legislation that is passed by Parliament.

Mr. Glen Motz: I'm done, then, Chair.

The Chair: Thank you, Mr. Motz.

Go ahead, Mr. McKinnon, please, for two and a half minutes.

Mr. Ron McKinnon: I do understand that you're a quasi-judicial body, and that limits what you can respond to here, but we're here to study Bill C-26 to make it better so that when it is delivered out into the world, it does its job. Is there anything you can offer us that will help us do that?

Ms. Leila Wright: What I can do is comment on the proposed amendments to the Telecommunications Act that touch on the CRTC's work. One of those proposed amendments is to allow the CRTC and other securities-focused government departments and agencies to share information in particular circumstances.

In other areas, we have the ability to share information among departments and agencies, and my colleague Steven Harroun can speak to some of the ways in which we have used that ability.

Mr. Steven Harroun: To build on Ms. Wright's comment, one of my roles in compliance and enforcement is with Canada's anti-spam legislation. In that legislation, there is very prescribed information sharing with my partners at the Office of the Privacy Commissioner and the Competition Bureau. We can share information as it relates to CASL and as it relates to our specific roles in enforcing that legislation, which has proven to be very effective.

Mr. Ron McKinnon: Thank you.

The Chair: Thank you.

That concludes our meeting today.

Mr. Doug Shipley: Sorry, I've been wondering about this. The Minister of Public Safety was scheduled to come to us for a two-hour discussion with regard to victims' rights. Do we have any idea when the minister will be coming for those two hours? That motion was agreed to quite a while ago.

The Chair: We'll follow up, Mr. Shipley. We're still waiting for an answer.

Mr. Doug Shipley: So are we.

Thank you.

The Chair: Thank you to the witnesses again.

Is the committee in agreement to adjourn the meeting? I want to be clear on this one.

Some hon. members: Agreed.

The Chair: Thank you.