HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

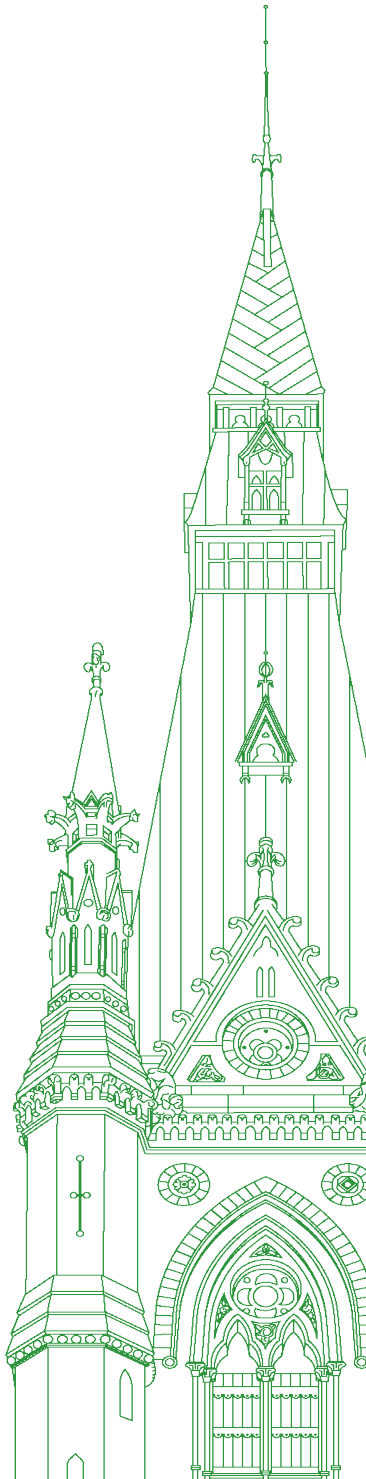
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 018

Thursday, December 4, 2025



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Thursday, December 4, 2025

● (1105)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ)): Good morning, everyone. I call this meeting to order.

Welcome to meeting No. 18 of the House of Commons Standing Committee on Public Safety and National Security.

Pursuant to Standing Order 108(2) and the House order of reference of October 3, 2025, the committee is meeting on its study of Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

Before welcoming the witnesses, since I am chairing today's meeting, I would like to ask for the consent of all committee members to maintain my privilege of having a six-minute turn to speak and another two minutes to ask questions of the witnesses.

Do I have the unanimous consent of the committee to do so?

Some hon. members: Agreed.

The Vice-Chair (Claude DeBellefeuille): Thank you.

I would now like to welcome the witnesses we have with us for the first hour of the meeting.

First, as an individual, we have Dr. Kate Robertson, senior research associate, Citizen Lab, University of Toronto. She is joining us by videoconference.

We also have with us John de Boer, who is vice-president of government relations at BlackBerry.

From OpenMedia, we have Matthew Hatfield, executive director, by videoconference.

Welcome to all of you.

We'll start with you, Ms. Robertson. You have five minutes for your opening remarks.

[*English*]

Kate Robertson (Senior Research Associate, Citizen Lab, University of Toronto, As an Individual): Good morning. Thank you.

My name is Kate Robertson. I'm a lawyer and currently a researcher at the University of Toronto's Citizen Lab.

My comments draw on Citizen Lab's research on cybersecurity and telecommunications, as well as constitutional law analysis that I submitted in a brief to this committee.

Parts two and three of my brief set out amendments to address constitutional deficits and cybersecurity risks in the bill. Out of those recommended changes, the introduction of the brief identifies two priorities.

The first is to explicitly protect encryption technology in Canada's telecommunications networks. At present, the broad powers in the bill could have the effect of compromising encryption standards for lawful access purposes.

For example, under proposed section 15.2 of part I of the bill, the minister could require that a telecom operator implement “specified standards”. The minister could prohibit a telecom operator “from using any specified product or service”. The minister could also “impose conditions on [the]...use of any product or service”. These are just some examples.

While officials have stipulated that this law is not a surveillance bill and that these provisions don't authorize the compromise of encryption, there is no explicit clause to ensure this. Future governments could interpret proposed section 15.2 very differently, arguing that heightened surveillance capabilities would promote Canada's security interests. An interpretive clause is essential to protect encryption, which is an essential form of cybersecurity.

I note in my brief that even the recently tabled Bill C-2, which also proposes very broad powers to order changes in telecom networks, has a specific clause that the government has pointed to as a proposed means of ensuring that orders won't compromise encryption. In contrast, there is still nothing comparable in Bill C-8.

Recommendation eight of my brief suggests that language should be added to stipulate that orders cannot be used to compromise the confidentiality, availability or integrity of a telecommunications service. This phrasing is a widely recognized term to describe the three essential elements of strong cybersecurity. It is a term that is used by federal agencies in Canada.

I can also answer questions about alternative language that would also be workable. I can submit those suggestions in writing after this hearing, if it's helpful.

Ultimately, since the intent of the legislation, as we've been told, is not surveillance or encryption-breaking, this should not be a controversial improvement to the bill.

As a second priority, the law's broad and warrantless collection power under proposed section 15.4 is a significant constitutional deficiency. As we know, telecom providers are conveyors of the most private information known to our legal system. I must respectfully disagree with the view that this law would only apply to technical information. The actual text of the legislation—which is what matters—creates a broad and warrantless power to collect personal and de-identified information from telecommunications companies.

I share the view of the intelligence commissioner of Canada—who has previously testified—that the warrantless search and seizure powers are a constitutional flaw in the bill with no apparent justification. I agree with Mr. Noël's recommendation that when it comes to the CSE specifically, an important change would be to require that the CSE's use of information be subject to annual ministerial authorization and, ultimately, approval by the intelligence commissioner. This would be a very notable improvement, but as he noted, there still would remain a warrantless collection flaw in Bill C-8 generally, which he testified is a problem that he would leave for others to address.

Recommendation three in my brief addresses this larger gap by proposing Federal Court authorization for the collection of personal and de-identified information. This is critical in order to place Bill C-8 on much stronger constitutional footing.

Given my time, I would invite a follow-up question from this committee on why the current safeguards in the bill, which are for the most part inapplicable to the collection power under section 15.4, are inadequate to remedying this constitutional deficit.

Thank you for your attention. I defer to my brief for my remaining recommendations.

● (1110)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Ms. Robertson.

We'll now go to you, Mr. de Boer. You have five minutes for your opening remarks.

John de Boer (Vice-President, Government Relations, BlackBerry): Thank you, Madam Chair.

[*English*]

When Canadians get into their cars, they trust that the safety-critical systems inside will work flawlessly. When industrial automation systems keep our energy grids running, we trust that they will perform as intended. That trust is what BlackBerry delivers every day.

Our QNX operating system is embedded in over 255 million vehicles on the road today. It powers industrial control systems, nuclear power stations and autonomous systems in mission-critical environments where safety, reliability and performance are non-negotiable. QNX is trusted to ensure that these systems are secure and reliable, because failure is not an option. Our responsibility does not stop there.

We protect the communications that keep leaders connected during a crisis and the systems that coordinate emergency response when every second counts. When a cyber-attack threatens a power grid and disrupts transportation networks or when a national security incident demands immediate action, BlackBerry ensures that sensitive information remains secure and that decision-makers can communicate without fear of interception or compromise.

Our mission is simple: safeguard the integrity of critical operations so governments and essential services can respond quickly and confidently. In these moments, trust isn't optional; it's everything. This is why banks, energy providers, telcos and transportation agencies rely on BlackBerry. We were built with security in mind from the ground up.

BlackBerry strongly supports Bill C-8, particularly part 2. Critical infrastructure is increasingly digital, making it a prime target for cybercriminals and state-sponsored actors.

The stakes are high. These systems deliver essential services and house sensitive data. A single breach can cascade across borders and sectors. Canada is the only G7 country without mandatory cyber-incident reporting for critical infrastructure. It's time we align and strengthen our cyber-defences.

Bill C-8 is a major step forward. It will enhance situational awareness and collective response, strengthen organizational learning to identify systemic risks and inform cyber-practices and improve corporate governance by elevating cybersecurity to the board level.

Global experience shows that these laws work. The United States' 2022 Cyber Incident Reporting for Critical Infrastructure Act has led to faster resource deployment, trend analysis and information sharing. Officials say it helps "spot adversary campaigns earlier, and take coordinated action". Europe's NIS2 Directive and Australia's Security of Critical Infrastructure Act show similar benefits.

Success depends on three factors. The first is speed. Rapid reporting enables rapid response. Second are clear definitions of what constitutes a reportable incident. Third is access to secure and certified incident reporting and critical event management tools that enable stakeholders to communicate in times of crises.

Canada needs this speed and clarity. The October 2025 Auditor General's report found that Canada's response to a major cyber-attack was delayed by seven days due to incomplete protocols and the lack of a tool for secure information sharing. That delay gave attackers more time to access sensitive information. Mandatory reporting must be paired with tools and procedures for seamless communication.

To make this law effective, we recommend five things. First, define “reportable incident” clearly and consistently. Second, mandate timely reporting with a tiered approach and initial notification within 72 hours followed by detailed reports. Third, provide access to secure tools for real-time communication and coordination. Fourth, guarantee liability protections for good-faith reporting. Fifth, include business continuity as a baseline requirement, ensuring entities can communicate, mobilize and restore services quickly.

In closing, Bill C-8 moves Canada from a patchwork of voluntary guidelines to a mandatory framework aligned with global best practices.

● (1115)

Thank you.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you.

I will now go to Matthew Hatfield from OpenMedia for five minutes.

[*English*]

Matthew Hatfield (Executive Director, OpenMedia): Good morning.

I'm Matt Hatfield, and I'm the executive director of OpenMedia, a grassroots community of 230,000 people in Canada who work together for an open, accessible and surveillance-free Internet. I'm joining you from the unceded land of the Tsawout on Salt Spring Island in British Columbia.

Loopholes matter. A bad loophole you pass in this legislation does not just weaken the law; it will prove far more important than the law's intended purpose. Right now, Bill C-8 contains several serious loopholes that you must fix.

Bill C-8 is built on and very closely resembles Bill C-26, the cybersecurity legislation this committee's predecessor passed last year. Both bills give future industry ministers the power to permanently and secretly disconnect Canadian citizens from the Internet without notifying them or explaining the decision; to issue orders to telecom companies to do or not do anything the minister says is necessary to protect our telecom infrastructure; and to keep you, our elected representatives, entirely in the dark about what these orders say. That is simply too much unchecked power. Canada does need cybersecurity legislation, but you should not pass this legislation as worded today.

In proposed subsection 15.2(2), the minister is given the power to order telecom providers to do anything or not do anything they believe is necessary to secure the Canadian telecommunications system. Constructively, Bill C-8 now states that the minister's use of these powers should be reasonable and within the act's purpose.

Who will decide if that standard is met? It's not the public; we're only informed of the existence of these orders in a yearly report. It's not your colleagues at NSICOP. The minister has to tell you only why they think what they're doing is reasonable, not show you that it is. That is not transparency and accountability; it is accountability theatre. The minister is required to think hard about whether their decisions are reasonable and proportionate and to promise you in writing that they are, but there's no oversight to check. This is much like a law that requires me to give you a very good explanation for why I think my hands should be in the cookie jar, but doesn't let you check what I'm actually doing in there.

Our democratic allies don't write legislation like this. In the U.K., the government cannot issue this kind of order without consulting Ofcom, the independent regulator. Different uses of order-making powers require the approval of an independent technical board, a reviewing judge or both. In Bill C-8, the minister alone decides.

In Australia, if a telecom company believes that an order would compromise the privacy or security of their network, they can demand a technical review by an independent judge and a technical expert. In Canada, the minister alone decides. Not coincidentally, these baked-in expert reviews also protect the government from accidentally creating technical disasters by issuing orders with consequences they don't understand that break rather than protect telecom infrastructure.

Canada's approach, Chair, is not a system of democratic checks and balances. It is a blank cheque to future government ministers to build a growing system of permanent secret orders whose reasonableness and proportionality is entirely in their hands, and the necessary fixes are really much like they were at the last stages of Bill C-26.

First, the government's new powers must be constrained by actual independent review. The minister's opinion that they are necessary and proportionate is not good enough. A judge and technical expert should have full access to these orders either before they are issued or, in emergency circumstances, within 30 days, and they should have the ability to overturn orders that go too far.

Second, Bill C-8's legitimate purpose is systemic infrastructure protection, not being misused to surveil Canadians. That means the bill must explicitly prohibit orders that have the effect of creating a systemic weakness or backdoor encryption, language already used by our allies in Australia. If the door is open for the minister, it is open for hackers too.

Further, personal information must be clearly defined as confidential and, if any is incidentally collected in the process of carrying out Bill C-8, it should be rapidly destroyed. In all circumstances, Bill C-8 must forbid personal information collected under it from being shared with foreign intelligence agencies that are not subject to our laws.

Third, the government must not be allowed to keep how it is using these new powers permanently secret, not from you and not from the public. Outside of immediate emergency situations, the standard of disclosure of what is happening under Bill C-8 should be one level higher than is currently required. That means that the public should be informed not just of how many orders are being made but of the minister's description of what they are accomplishing and why they are necessary. NSICOP should be provided with a full description of the orders so MPs can judge if the minister's public report is telling Canadians the truth.

More than 10,000 Canadians have written to our government to demand this cybersecurity legislation pass only once it includes robust rights protection. That's your job to do. We urge you to listen to these voters and to adopt the amendments that civil society has placed before you to get this legislation to where it needs to be.

Thank you, and I look forward to your questions.

● (1120)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Hatfield.

I'd like to thank the witnesses for their presentations.

We will now go to questions from members. We'll start with Mr. Lloyd for six minutes.

[*English*]

Dane Lloyd (Parkland, CPC): Thank you.

Thank you to all the witnesses for being here today.

I'm going to start with a question for you, Mr. Hatfield.

You said there really isn't any oversight when the minister makes a decision, and the bill says that it has to be a reasonable decision. Given that these powers would primarily impact telecom providers, but possibly in some cases individuals, as has been claimed, can these people not seek judicial review of these decisions, and if a judge finds that they aren't reasonable, have these order overturned? Is that not a safeguard?

Matthew Hatfield: I would defer it to my colleague, Kate, for a lawyer's view on this.

This is a public advocacy perspective for me.

If someone eventually has a decision overturned, it could be months or years before it's changed. Many people in Canada, of course, wouldn't have the resources or understanding to challenge these orders. I don't think it's nearly as good as having a built-in process the government is forced to go through to seek a later process.

Kate Robertson: Under the Constitution, the courts will look for a meaningful system of accountability. If you have an absence of transparency, a notice to individuals, including potentially the need for strict gag orders that would prevent individuals from knowing that their privacy, or other interests, have been impacted, then that thwarts their ability to meaningfully access review mechanisms. In that regard, the judicial review is inadequate from a constitutional perspective.

I'd also note that there is a reasonable best standard, and there's deference applied, which is why I recommended that we have a specific clause clarifying that this is essentially not for surveillance purposes but is about cybersecurity, because that as well would be, in the absence of such an interpretive clause, assessed on a different standard in the judicial review process.

● (1125)

Dane Lloyd: Ms. Robertson, I was told by witnesses from the Canadian Constitution Foundation that even if there's a secret order placed on somebody, they still have their right to seek a judicial review. Is that not the case?

Kate Robertson: That's the case, but if they aren't themselves within the cone of the gag order, then they wouldn't know of the existence of government orders or subsequent action by telecom providers.

Dane Lloyd: We were told by the department that anyone who is impacted by these orders is informed that they're impacted by these orders. Is that not the case?

Kate Robertson: That's not the case, and it really depends on the specific nature of the order itself. There are many ways that this bill suggests that from the minister's perspective in introducing this legislation, they see this as a matter between telecom providers and the government. In many ways the public at large is, I have to say, treated as not part of the equation. If there is an order that's specific to an individual, that would be a different matter, but for many cases, the intent of the legislation and how it's been discussed appears to be really looking at orders to telecom providers, and in that way individuals would not receive notice.

Dane Lloyd: I want to switch gears here and talk about the encryption rules. What stakeholders would be most concerned about the potential that encryption would be broken by this legislation? Would it be stakeholders like BlackBerry here today?

Kate Robertson: It certainly could.

I would commend the 2017 CBC investigation that showed that in the case of a member of Parliament, once an investigative journalist gave a security researcher that member of Parliament's phone number, the security researcher—in this case consensually, but it will illustrate the problem—was able to intercept that member of Parliament's locations, text messages and communications. That really shows the systemic vulnerabilities that are inherent in the world's mobile communication networks, and that's what we hope 5G and 6G technology will help us with, including through the introduction of robust security features including encryption.

Dane Lloyd: Thank you. Sorry, I do have a limited amount of time here.

Mr. de Boer, you're here representing a telecommunications stakeholder. I'm wondering why the encryptions haven't been raised as a concern in your testimony today. Is that a concern you have, and can you elaborate on those concerns?

John de Boer: From a BlackBerry perspective, I think the notion of reasonableness is very important and the notion of judicial review, but we are no longer in the telecommunications business.

Dane Lloyd: Okay.

John de Boer: Our focus is more around cybersecurity.

Dane Lloyd: Do you deal with encryption at BlackBerry?

John de Boer: We do deal with encryption.

Dane Lloyd: Are you concerned that provisions in Bill C-8 would allow the government to thwart your encryption, or legally force you to break your encryption standards?

John de Boer: We will be concerned if that actually comes to bear, but we would like to have judicial review and the right for reasonableness.

Dane Lloyd: Do you think the provisions in this legislation give the government the power to do that?

John de Boer: I'm not in a position to really opine on that. It's not my area of focus.

Dane Lloyd: That's a big concern that's been raised by many stakeholders. Theoretically, if the government came to you and gave an order that your company felt would break your encryption standards, what would be the response from your company?

John de Boer: It would be problematic.

Dane Lloyd: Would it seek a judicial review for the decision before complying with the decision or...?

John de Boer: It would be case by case. I can't comment on a fictitious scenario, but we would definitely review that.

Dane Lloyd: Yes, it's been painted as a very real scenario by many witnesses, and it is concerning. Thank you for that.

I don't know if you could provide any briefings to this committee afterwards. If you could get that information—

John de Boer: I'm happy to do that.

Dane Lloyd: —that would really help the committee.

Thank you.

I think that's all my time.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Lloyd. You're making my life easy by stopping a little before your time is up.

I now give the floor to Ms. Acan for six minutes.

Sima Acan (Oakville West, Lib.): Thank you, Madam Chair.

[*English*]

Mr. de Boer, I have an engineering degree in electronics engineering, and my focus was telecommunications. Throughout the years, I was in industrial automation, which you mentioned, and robotics, where communication and cybersecurity were at the core. That's why my questions will be for you.

You previously testified in support of the objectives of the predecessor to this bill, Bill C-26. Given the scale of cyber-threats to essential services, can you elaborate on why a legislative framework like Bill C-8 is necessary for Canada's cybersecurity posture, particularly within the federally regulated telecommunications sector?

● (1130)

John de Boer: You know, as I stated in my testimony, Canada's the only G7 country without a mandatory cyber-incident reporting bill or a cybersecurity program for critical infrastructure. This has been a long time coming. The threat landscape has evolved significantly, so in order to actually protect critical services, it is absolutely essential.

This is a start. We're focusing on four federally regulated sectors here, but we know that similar approaches need to be taken in other critical sectors as well.

The reality is that Canada works closely with its allies. We have Five Eyes allies and others. If they see us out of step, if they see that our critical infrastructure is not adequately protected, then that could also erode trust in our systems. So, I think it's very important.

Sima Acan: Thank you very much.

You actually lead into my second question.

You have advocated for harmonizing Canada's cybersecurity framework with Five Eyes partners. Beyond just compliance and incident reporting, what specific mechanisms adopted by other jurisdictions—like the U.K., Australia or the U.S.—that are related to balancing operational security needs with transparency should Canada adopt to strengthen Bill C-8?

John de Boer: One area that may be of interest would be, first of all, ensuring liability protection for good-faith reporting. That needs to be strengthened within this bill to align with, for instance, the United States and also the EU and Australia.

With regard to other incidents, things we could clarify would be what kind of cyber-incident would qualify under the reporting. Currently, as it's defined in this bill, it's any incident that affects the continuity or security of a vital system. In the United States, in Europe and in Australia, they've added “significant” to it. I think there needs to be further.... I know this will be outlined in regulations, but it's important that we make certain distinctions.

Sima Acan: Thank you.

From the perspective of a technology company serving both government and the private sector, how do you perceive the necessity of expanded government regulation and security-critical infrastructure, and how does this duty balance with the responsibilities borne by private, designated operators under the proposed critical cyber-systems protection act?

John de Boer: In order to respond effectively, and I think the Canadian government has made some strides here, it needs to be a public-private partnership. There is an onus also on the private sector to ensure that their products are secure and meet a standard that is acceptable for critical infrastructure in particular. Notions like “secure by design” are really important in understanding third party supply chain security risks. For BlackBerry, this is why we take certifications of our products very seriously. We get certifications from national authorities to ensure that our products are approved products.

I think it's really critical that the Government of Canada signal to critical infrastructure and the rest of Canada that it's important to use products that are secure, and that private industry also work to build secure products instead of just immediately releasing products that may have flaws contained in them. Bolting on security after the fact does not work.

Sima Acan: Thank you very much.

Do I have time, Madam Chair? Okay.

In your previous testimony on Bill C-26, you specifically recommended that Bill C-8 harmonize cyber-incident reporting requirements with Five Eyes nations, as you mentioned. One of the objectives of Bill C-8 is to modernize our cybersecurity framework with those partners. Could you speak to how this legislation aligns now with Five Eyes partners in relation to incident reporting and compliance?

John de Boer: Absolutely. With respect to incident reporting and compliance, as I mentioned in my testimony, in the United States there is mandatory cyber-incident reporting covering 16 critical infrastructure sectors. They must be reported within 24—

● (1135)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I'm sorry to interrupt you, Mr. de Boer, but Ms. Acan's time is up. You can finish your answer in another round.

It's now my turn to have six minutes to ask the witnesses a few questions, as agreed.

My first question is for Ms. Robertson.

We heard from the Privacy Commissioner about the principles of necessity and proportionality when it comes to collecting and sharing personal information. These are principles found in many acts, but they are not systematically included in Bill C-8.

What do you think about systematically introducing these principles into Bill C-8?

[*English*]

Kate Robertson: I couldn't agree more with the Privacy Commissioner of Canada's remarks. I agree to the extent that the same suggestions are included in my brief under recommendation five.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Excuse me, Ms. Robertson, but I see that the French interpretation is not working. As chair of the meeting, I have to interrupt you to point that out.

[*English*]

The Clerk of the Committee (Andrew Wilson): I just want to test to see if the translation is working in French.

It works. Thank you.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you.

Could you repeat your answer, Ms. Robertson?

[*English*]

Kate Robertson: My apologies for not being able to answer in French.

As I indicated, I completely agree with the Privacy Commissioner of Canada's remarks on the importance of this amendment to the legislation. It is included in one aspect but not comprehensively, as you noted. This is one of the really significant constitutional deficits I identified in relation to proposed section 15.4 of the legislation, which is the collection power.

Recommendation five in my brief also addresses precisely the same issue as the Privacy Commissioner of Canada testified to. I would link that not only to the privacy framework that the commissioner is responsible for but also to the constitutional principles that I've analyzed and that apply in this context.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): In your presentation, you told us about your concerns with proposed section 15.2 of the bill. The section could be used to create back doors and ultimately weaken encryption standards. I am not a computer scientist, but I understand that it is currently difficult to break into the systems, since the encryption standard is very high. Lowering that standard could be a security risk.

Have I understood your argument correctly?

[*English*]

Kate Robertson: Yes, you understood it very well. The only clarification I would make is that traditional telecommunication technology was insecure by design, and with legacy mobile communication networks we still see persisting vulnerabilities that make people vulnerable to cyber-fraud and other types of malicious surveillance, such as corporate espionage, for example, and espionage of government officials.

We have security features, including encryption, available for 5G and 6G technology, but we know, for example, that in Europe there has been some lobbying by law enforcement to disable these privacy-enhancing technologies in order to enable easier forms of law enforcement surveillance, which of course is the exact opposite of what we want and what we desperately need to make sure our systems are secure by design and not insecure by design.

We need to be fixing as many holes as possible. as opposed to drilling new holes, and that's why I take it that government officials have agreed that this bill is not about surveillance and not about encryption-breaking, but we can only know that if we have that encoded in the law itself, which is a gap that we urgently recommend be filled.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Ms. Robertson, did you have a chance to testify on Bill C-26? Were these concerns discussed and debated?

Have you had a chance to make the government aware of the weakness in Bill C-8, which was also in Bill C-26, and to let them know that it could cause harm and even promote cyber-attacks?

● (1140)

[*English*]

Kate Robertson: The issue is that there are multiple interpretations about how these orders may be issued, and we would like them to be as transparent and accountable as possible, because some may view encryption-breaking as a way to make Canada more secure, but we know that's not the case.

The combination right now of interpretive ambiguity and a potential that these orders are issued in secret makes it particularly worrisome that these new security features will be compromised by potentially—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I'm sorry to interrupt you, Ms. Roberston, but it seems that there is no longer any interpretation.

This is extremely distressing for both of us.

[*English*]

The Clerk: I just want to test again that the French interpreter is back on the French channel.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): It's working now.

I apologize for that little constraint on us, Ms. Robertson. It's because the interpreters are working remotely. That's an additional obstacle to interpreting your remarks.

You may now continue.

[*English*]

Kate Robertson: Yes, I was testifying that with the combination of secrecy and lack of clarity these orders could be used to compromise encryption, and that is a problem.

I would also note that it's not difficult to foresee that these orders might be used for surveillance capabilities. The Ministry of Public Safety has introduced legislation for this exact purpose of installing new capabilities in telecommunications systems, but of course that should be under its own legislation if it's going to happen and attached to very different sets of safeguards. This bill is about cybersecurity, and not about surveillance, as we are told, which is why we need to ensure these types of compromises aren't coming in through Bill C-8 itself.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Ms. Robertson.

Colleagues, since we started the meeting late, we have a decision to make. The first option would be to start the next round as planned by giving the floor to Mr. Au, Mr. Ehsassi and me, but Mr. Caputo and Mr. Powlowski would not have their turn to speak. The other option would be to agree to adjourn the meeting later to allow committee members to speak in the usual order.

Do you want to add 15 to 20 minutes to the meeting or do you want to reduce the time you have to ask your questions?

A voice: We can adjourn later.

The Vice-Chair (Claude DeBellefeuille): I see you agree that the meeting should adjourn around 1:20 p.m. It would adjourn at 1:17, to be precise.

We'll now go to the second round.

Mr. Au, you have the floor for five minutes.

[*English*]

Chak Au (Richmond Centre—Marpole, CPC): Thank you very much.

I want to direct my questions to Mr. de Boer.

I agree with you one 100% when you say that trust is important in the sense of being secure and reliable. You also mentioned that we are the only G7 country lagging behind, so my first question is, in comparison to other G7 countries, how far behind are we, and what is the significance of that kind of lagging behind?

John de Boer: The United States passed a similar law in 2022, so almost four years ago. In Europe, an NIS2 directive was enacted last October, while Japan enacted one in April and Australia did so last year, so we're at least one to four years behind our peers, essentially, and that makes us vulnerable.

Chak Au: In that case, do you think the lagging behind is intentional, or is it negligence?

John de Boer: I wouldn't say it's intentional. I know the government has tried to work on this bill and pass this bill for a while. It's taking time to get it right.

Also, our federal system makes things difficult, but I would stress that the urgency is now. We need to get this done. Cybersecurity is probably one of the most prevalent threats we face today.

● (1145)

Chak Au: Very good.

To follow up, sometimes I hate to hear the words, “This is a step in the right direction” or “This is a good first step.”

How many steps do we have to take in order to get to the destination we want to arrive at? What is your recommendation? How can we approach the destination faster?

John de Boer: I see this as a first step because, first of all, it deals with four critical infrastructure sectors. We have many more than that. Even the notion of what is critical infrastructure is changing. It's taken Public Safety Canada years to come up with a new critical infrastructure strategy.

This is going to be an ever-evolving assessment. It's really important that we continue to expand applicability of these kinds of requirements beyond just the four sectors. There also needs to be a harmonized approach with provinces and territories.

Unfortunately, threat actors are finding new ways to attack our critical infrastructure. We need to adapt and be ready to adapt.

Chak Au: In other words, how can we be more proactive instead of always trying to catch up? What do you recommend?

John de Boer: One core thing I can recommend is to strengthen public-private partnerships. Work more closely with companies like BlackBerry and other companies that have a lot more knowledge, in some cases, of the threat actors that are attacking critical infrastructure. We see them day in and day out. The Canadian government can only do so much.

One initiative that the Canadian government is moving forward is called the Canadian cyber-defence collective, which is a good initiative that will bring together public and private sector entities to deal with immediate crises and medium-term crises.

That's a good first step.

Chak Au: It's another good first step.

In your report, you mentioned a large volume of cyber-attacks—five million cyber-attacks in three months—so it's a serious problem.

Do you feel that the current Bill C-8 would help you and your company to address those cyber-attacks?

John de Boer: Information sharing is really important. Understanding how the threat is evolving, what the trends are and what kinds of tactics and procedures threat actors are using help you build defences down the road.

Part of what Bill C-8 does is mandate information sharing in a confidential way. If you know what the enemy is doing or what rogue actors are doing, you can better prepare, so yes, the short answer to your question is it will help BlackBerry and it will help our customers. It will help us evolve our technology to higher encryption standards, etc.

It's very important.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. de Boer.

I now give the floor to Mr. Ehsassi for five minutes.

[*English*]

Hon. Ali Ehsassi (Willowdale, Lib.): Thank you, Madam Chair.

Thank you to our witnesses. This has been very helpful.

I'll start off with Mr. de Boer.

You have emphasized the need for private-public partnerships on several occasions today, and you've also noted that we're behind our Five Eyes partners.

Do any of the other Five Eyes partners use private-public partnerships?

John de Boer: Yes. In the United States about three years ago, they came out with the joint cyber-defence collective, which brings together private industry and public industry. In the U.K. they've had that for over five years, and the same in Australia. The good news is that Canada has also joined something called the International Counter Ransomware Initiative, which BlackBerry co-chairs in a public-private partnership.

These steps of working closely with the private sector have now begun in earnest. It does exist in other countries.

Hon. Ali Ehsassi: Is that a consultative process?

John de Boer: It's not just consultative. In some cases, it's joint action to take down actors and to deal with and respond to active cyber-threats as well.

Hon. Ali Ehsassi: Okay. Thank you for that.

Your third recommendation was that we provide access to security tools. Can you elaborate on that?

● (1150)

John de Boer: As was discussed in the Auditor General's report in October, even if you have a clear mandate to share information, if you don't have a means to effectively communicate it to those who need it, then you're stuck. Currently, according to that report, the Government of Canada does not have a sanctioned tool to be able to share information effectively. At BlackBerry we specialize in this area of work. What's important for us is to ensure that whoever is sharing information is doing it in a secure means, not using commercial apps or apps that were not built for exchanging secure information.

Our recommendation would be to find a way, a tool, and leverage that across critical infrastructure and government in a unified way, using tools that are certified for that purpose and that are approved specifically for sharing information.

Hon. Ali Ehsassi: Thank you very much.

I'll go now to Ms. Robertson.

Thank you very much, Ms. Robertson. I take it that overall, without getting into the details, you are very much in favour of Bill C-8. Is that correct?

Kate Robertson: We welcome a more proactive approach by the government. As we note in our research, legacy, lack of accountability and excessive secrecy have actually led to—

Hon. Ali Ehsassi: Generally—not specifically, but overall—you appreciate that we're behind our other Five Eyes partners and it's important that we do address this issue. Is that correct?

Kate Robertson: My testimony is that the government does need to take a more proactive role. However, it has been unfortunately complicit in some of the surveillance technologies that have made these technologies insecure in the first place. We really need to see—

Hon. Ali Ehsassi: That doesn't really answer my question. Thank you.

Kate Robertson: Well, it does answer it from my perspective. That's my view.

Hon. Ali Ehsassi: No, I understand that you don't agree with certain provisions. That's understood. But for you not to answer whether you think Bill C-8 as a general rule is moving in the right direction.... That's essentially what I was asking.

Kate Robertson: I've been asked this before. I think this is about a long-term strategy. It's not a rapid response. There are other tools for that. I would prefer, and it's my view, that they should proceed with amendments as opposed to just proceed because we're operating from a place of fear.

Hon. Ali Ehsassi: Thank you. This is not a rapid response, as we've heard from numerous witnesses. We're way behind our other Five Eyes partners. No one is suggesting that this is a rapid response. But you do agree, Ms. Robertson, that there will be judicial review for any decision that is taken by the minister. Is that correct?

Kate Robertson: No. I don't agree with that. It's only if a party initiates a judicial review. Of course, if there's secrecy—

Hon. Ali Ehsassi: But the right is there. It is secure. You agree with that, I take it.

Kate Robertson: It's impossible to access it if we don't know that the government order has been issued or what its effect would be. So if—

Hon. Ali Ehsassi: Thank you. You're saying that the people it applies to may not very well know about their—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Ehsassi. This is very worthwhile and fascinating. We can continue this discussion later.

It's now my turn for two and a half minutes.

Mr. Hatfield, in your opinion, does the bill provide a mechanism for monitoring cabinet orders on cybersecurity? Do you think it's enough? Would the bill need to be amended to provide better oversight of the minister's power?

[*English*]

Matthew Hatfield: Yes, very much so.

I'll answer the question that was just asked: Should Bill C-8 pass in its current form? No. Should it pass in some form? Yes, potentially, if the right amendments are brought in.

It's true that our cybersecurity protections and legislation are behind those of our allies. Why are we considering legislation, then, with much weaker oversight than our allies apply? I think that's the crucial step that needs to be addressed here. The minister, alone, cannot be making these decisions. Our right to judicial review, which occurs only when we find out about the impact of a secret order that we've never seen, isn't a real right at all.

There are various bodies that could be appropriately empowered to provide oversight here. We could see NSICOP provided with much more information about what's going on in these orders so that they can judge that. However, the public needs to have a clearer view of what's going on systemically with the system as well, otherwise you could have secret orders stacked on secret orders and have a growing system that could become, really, far more about surveillance than about cybersecurity.

● (1155)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Do you intend to suggest amendments to provide better oversight of the minister's powers? You may not have them at your fingertips, but is that something you could send to the committee, Mr. Hatfield and Ms. Robertson, to better enlighten us?

[*English*]

Matthew Hatfield: Yes, certainly.

I can say some of them briefly now: no permanent secrecy; automatic review of orders, of secret information, by an external party, at some point; more reporting to the public on what's going on; as well as additional protections around encryption and preventing systemic weaknesses in the system.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you.

We'll now go to Mr. Caputo for five minutes.

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you, Madam Chair.

Welcome to the chair.

[*English*]

I would like to thank all of the witnesses—the two virtually and the one in person—for being here.

I want to start off with Professor Robertson.

First of all, your brief is incredibly comprehensive. I thank you for something so voluminous and so precise.

It's not lost on me that I've often been criticized at this committee for interrupting officials, like the minister, yet you were interrupted repeatedly when the answers you were giving may not have been what some people at the committee would have wanted.

I'm going to let you take this time to complete any answers to questions that were asked. If you have anything to add, please feel free to add it at this time.

Kate Robertson: Thank you very much.

If I could quote the remarks of Canada's intelligence commissioner, “The glaring absentee in [this legislation] is the Canadian public”, whose information, which is the subject of a reasonable expectation of privacy, is under threat of compromise in more ways than one in the legislation.

We would very much welcome the government taking a more proactive approach in ensuring that we have network-wide security standards that protect you, me and everyone watching this hearing, and their communications.

When we have raised the constitutional deficiencies around the privacy risks and cybersecurity risks, we note that the government has taken the position that this is a regulatory context where privacy interests are diminished. However, we know that the privacy interests of the individuals who use telecommunications are not in any way diminished. Human communication is not a regulatory matter. That's why we point out that the balancing exercise that's critical to protect privacy and security, in this case, is not meeting the mark.

You have recommendations from me—nine in total. We believe that these are entirely consistent with the government's purpose of the legislation, which actually creates a corresponding risk that, if available improvements are not taken, then the courts are that much more unable to understand why a constitutional violation is reasonably justified. That just really kicks the can down the road to entanglements in the courts when unconstitutional legislation is not appropriately amended to address those issues.

Frank Caputo: Thank you. I was going to ask you at some point about the charter, but you've outlined that fairly clearly.

For now, what I'd like to do is propose.... Any of the witnesses can feel free to weigh in on this. I don't believe that the bill has a sunset clause. I think that this bill has been quite controversial. I'm hearing about it as critic and we are hearing about it at committee. The general consensus has been—and not everybody has said this—that there is a necessity for legislation on this topic. I'm paraphrasing you, Professor, that we shouldn't be passing this legislation carte blanche and without scrutiny.

As I would say in my legal career, it's not just important that we get it done; it's that we get it right, especially on something like this.

One mechanism is a sunset clause. I'd love for each of you, or whoever wishes, to weigh in. I suppose a sunset clause can take multiple forms. One of them is a review at committee after five years, which in my experience doesn't generally happen. It just gets kicked down the road. Another would be a legislative review. I'm not sure if or how that would occur, but I suppose we could fashion that. Another is the bill just sunsets after three years. In other words, you need new legislation to revive it.

Do any of you have opinions on that?

Mr. Hatfield, please go ahead.

● (1200)

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Wait, Mr. Hatfield, I think there's a technical issue. I don't think the audio in the room is working properly. We'll check it.

[*English*]

The Clerk: Mr. Hatfield, can you just speak for a few seconds? I want to see if there's an issue with the room sound.

Frank Caputo: Mr. Hatfield, could you please repeat what your answer was? After that, Professor Robertson and Mr. de Boer, you can offer any thoughts, please.

Matthew Hatfield: [*Technical difficulty—Editor*] with the sunset clause currently is that MPs aren't being provided with the information that you will need to judge the operation three or five years from now. The government is holding too much secret information or just having the minister say what it believes to be reasonable. You need far more information to be able to make a meaningful decision there.

Frank Caputo: Professor, do you have any thoughts?

Kate Robertson: I'm a lawyer and researcher at the University of Toronto, but I don't hold the title of professor, so I'll just clarify that.

In my view, we've had the unique opportunity to hear from a former Federal Court judge who's been very explicit, if I could put it that way, in saying that there is a constitutional vulnerability here for which she sees no justification.

Of course, I agree with that assessment from my own perspective, but when you have the clarity of the issues put in such a crystallized—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I'm very sorry, but I have to interrupt you here.

That is the end of this round of questions for the witnesses.

No, it's true, you still have your turn, Dr. Powlowski. I was forgetting you. I apologize profusely. Can you forgive your young, almost 62-year-old chair for the omission?

[*English*]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): It's no problem.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): It's over to you, Dr. Powlowski, for five minutes.

[*English*]

Marcus Powlowski: Maybe you're going to be disappointed with the quality of my questions. I'm certainly no expert in this. I'm new to Bill C-8 and new to this committee. I have a general question and then maybe I'll pass it on to Mr. Ehsassi.

It seems to me that the purpose of this legislation is to be able to detect and rapidly respond to cybersecurity incidents when bad actors like the Russians or Chinese are trying to interfere with some vital sectors within our society, which certainly seems to be happening. It seems to be a modern part of international warfare.

I would think, Ms. Robertson and Mr. Hatfield, that your concerns are over adequate protections of various people in society, but is there not a compromise that you're looking for here in terms of...we have to respond rapidly, as Mr. de Boer has said, when there is a cyber-incident. If we clutter this up with a lot of.... Perhaps that's not a good word. If the requirements and protections for civil society are too onerous, does that not potentially compromise our ability to react quickly to cyber-threats? Wouldn't this be exactly what Mr. Putin would like—to put so many different layers of protection in there that it takes days to actually be given the legal ability to respond to this?

I see a hand up. Ms. Robertson, you look like you're eager to respond to this, too. Why don't you start and then we'll go to Mr. Hatfield.

● (1205)

Kate Robertson: We have an interpretive disagreement. I understand government officials agree that we shouldn't be breaking encryption, but what we're recommending be changed is that we confirm this explicitly. In some ways, this is about interpretation and not procedure and due process.

Even if you take my example of Federal Court authorization of the collection of personal information and de-identified information, those authorization procedures always include an exigent circumstance, as a clause, when there is an emergency that needs to be addressed. That's why I say my recommendations—

Marcus Powlowski: I'm sorry, but could you explain the exigence clause? What exactly is that?

Kate Robertson: It means that if the government normally has to obtain authorization from a judge to obtain information, that's the subject of a reasonable expectation of privacy, as pretty much all information in the possession of telecommunications providers is personal information. That authorization isn't necessary when there's an emergency: “Exigent circumstances” is a legal term for, “It's an emergency, and we need this information now.” That, however, shouldn't be the default rule, so that's why we say that authorization should be required. It would be not at all thwarting the ability of the government to rapidly respond, when required.

Marcus Powlowski: Go ahead, Mr. Hatfield.

Matthew Hatfield: We're looking for review after the fact, when emergency orders are necessary. It's possible that something happens immediately, and the minister has to respond and get something done right away. Sure, that's fine. Review, in that case, should occur within 30 or 60 days, so that a judge and technical expert can take a look to make sure the order was reasonable and, potentially, should continue longer than just that emergency term. A common expression in privacy and security is, “Trust, but verify.” We're looking for some initial extension of trust to the minister but then verification that the purpose of the bill is being followed.

Marcus Powlowski: Ali, go ahead.

Hon. Ali Ehsassi: Thank you.

I want to ask a follow-up question to Ms. Robertson. Ms. Robertson, you talked about how there is interpretive ambiguity. It seems to me that interpretive ambiguity is always there until regulations are adopted with greater specificity. Would you not agree with that?

Kate Robertson: I don't agree with that. The failure of a piece of legislation to adequately circumscribe surveillance or information collection capabilities of a broad scope is actually cause, in and of itself, for the courts to strike it down, and that's exactly the problem we have right now. The government has indicated, in response, that it doesn't intend to use the legislation in a certain way. However, assurances are not an appropriate basis to delimit legislation. I cite the 2024 special report of NSIRA, which actually pointed out, in one of the last examples of national security laws being overhauled, that one of the national security agencies had testified, in a study committee, that—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Ms. Robertson. I'm sorry for interrupting, but Mr. Ehsassi's time is now up.

If I'm not mistaken, this is now the right time to thank you for your testimony. It will help all committee members study the bill in greater depth.

Mr. de Boer, thank you for coming to be with us in person.

We will now suspend the meeting to welcome the next panel of witnesses.

● (1205)

(Pause)

● (1210)

The Vice-Chair (Claude DeBellefeuille): We are resuming the meeting.

We welcome the witnesses. I would like to thank them very much for having travelled here to take part in the meeting in person.

First of all, we have Todd Warnell, who is chief information security officer at Bruce Power.

From Electricity Canada, we have Francis Bradley, president and chief executive officer.

Welcome.

You will each have five minutes for your opening remarks.

We'll start with Todd Warnell.

[*English*]

Todd Warnell (Chief Information Security Officer, Bruce Power): Thank you, Madam Chair and members of the committee. My name is Todd Warnell. I am chief information security officer at Bruce Power, Canada's only private sector nuclear operator. Since 2001, Bruce Power has delivered about one-third of Ontario's electricity, and it produces life-saving medical isotopes used around the world to fight cancer.

I appreciate the opportunity to participate in your review of Bill C-8. Today I will focus on why it is imperative to proceed with this legislation, particularly part 2, the critical cyber systems protection act.

Canada's critical infrastructure is facing unprecedented cyber-threats that put the safety, reliability and daily lives of Canadians at risk. Bill C-8 is a pivotal first step to strengthening our collective resilience and securing essential services. This legislation is more than policy; it is a commitment to protect the backbone of our economy and national security in a rapidly evolving global threat landscape.

Within Canada's nuclear industry, we have demonstrated that through collaboration with government, regulators, industry, academia and individual Canadians, we can successfully establish and regulate cyber systems that are crucial to the safe and reliable operation of critical services.

Bill C-8 aims to secure essential systems, encourage proactive risk management and enable responsible government intervention in cases of significant cyber-threat.

The critical cyber systems protection act will introduce a broad framework from which all critical sectors, in collaboration with government and the regulators, can develop and implement risk-informed and performance-based regulations to enhance the reliability and resilience of critical services.

Recent publicly released information about Canadian and allied intelligence agencies has made it very clear that nation states and cybercriminal organizations are actively pre-positioning within critical infrastructure in Canada and beyond. These threat actors are preparing for disruptive and potentially destructive actions targeting essential services that Canadians rely upon daily. The Canadian centre for cybersecurity, as well as allied agencies such as the United Kingdom's national cybersecurity centre have issued stark public warnings about the increasing sophistication and persistence of these threats. The urgency to act is underscored by real-world incidents and ongoing campaigns that demonstrate both the capability and intent of adversaries to disrupt or damage critical infrastructure.

I will review a few key points on the benefits of moving forward on Bill C-8.

Number one is strengthening national security and safety. Bill C-8 is crucial for protecting national security by requiring private and public organizations within critical infrastructure to adopt robust cybersecurity practices. As cyber-threats evolve and become more sophisticated, securing critical infrastructure and services is paramount to national security and public safety.

Number two is enhanced risk management. By enforcing mandatory risk management practices, the bill would help organizations move away from a reactive posture to a proactive approach that minimizes risks before they escalate into actual incidents.

Number three is government authority in high-risk scenarios. Bill C-8 would give government the authority to act swiftly during severe threats to critical infrastructure, protecting essential services and public trust. To further strengthen the effectiveness of the approach, it would be beneficial for Bill C-8 to provide greater clarity and distinction between the role of the Canadian Centre for Cyber Security as the technical authority and the responsibilities of sector regulators. Clear separation of these roles will help ensure coordinated, efficient and expert-led responses to cyber-threats across Canada's critical infrastructure sectors.

Number four is alignment with our global allies. Our allies are implementing or have already implemented similar cybersecurity laws. Bill C-8 would allow Canada to align with international partners and make it easier for Canadian companies to operate globally within secure frameworks.

Last is economic security. Cyber-attacks on critical sectors have far-reaching economic implications. By ensuring that key industries and services are protected, Canada would also safeguard its economic stability, helping to prevent cascading consequences that could arise from disrupted services and infrastructure.

In conclusion, Bill C-8 is a well-intentioned and urgently needed step to address the pressing issue of cybersecurity in Canada and in Canada's critical infrastructure sectors. The threat environment has dramatically evolved, and the threats are no longer theoretical. Action is required now to protect Canadians and our allies.

● (1215)

Thank you for the opportunity to address the committee. I look forward to your questions.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Warnell.

I now give the floor to Mr. Bradley for five minutes.

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

My name is Francis Bradley, and I'm the president and chief executive officer of Electricity Canada.

Electricity Canada is the national voice for electricity in the country.

The Vice-Chair (Claude DeBellefeuille): Excuse me, Mr. Bradley. It seems there's a problem with the interpretation.

[*English*]

Sima Acan: There are something like three other English voices on the same channel.

[*Translation*]

The Clerk: We're going to do a test. Can you hear me only in English on the English channel?

The Vice-Chair (Claude DeBellefeuille): I think it's working for everyone now.

You can start your introduction again, Mr. Bradley.

Francis Bradley: Thank you.

Electricity Canada is the national voice for electricity in the country. Our members generate, transmit and distribute electricity in every province and territory.

Thank you very much for inviting me to testify on Bill C-8. Last December, I testified before a committee of the other chamber about Bill C-26.

The new cybersecurity obligations in Bill C-8 apply to certain critical infrastructure under federal jurisdiction. In our sector, it's mostly international and interprovincial transmission lines, as well as nuclear power plants. Like several other witnesses, we recognize that there is a legislative gap in Canada's approach to cybersecurity. We therefore support the overall objectives of the bill. However, we do have some concerns, and we are proposing some amendments to better protect existing partnerships with federal agencies and enhance the security of our sector.

● (1220)

[*English*]

First, we recommend that Bill C-8 be amended to introduce clear protections and safe harbour provisions for organizations that voluntarily disclose cyber-incidents or vulnerabilities to the government. These protections should ensure that information shared in good faith by organizations is not used to initiate lawsuits or regulatory penalties. In our view, the absence of such protections is a major gap. Without them, operators will likely receive legal advice to share only the minimum information required to comply with the act, and nothing more.

As I discussed with regard to Bill C-26 on the same issue, this would result in a chilling effect on information sharing. This would be a missed opportunity to foster open collaboration and information sharing with government, both of which are essential to strengthening our collective resiliency.

A second concern relates to the potential risks Bill C-8 poses to the partnerships that critical infrastructure operators currently maintain with CSE's cyber centre. Today, our sector benefits from a collaborative relationship with the cyber centre, grounded in the confidence that information shared with it is not disclosed to regulators, enforcement bodies or other departments.

Bill C-8 could change this. It would require that CSE share incident reports with regulators, provide advice or services to regulators on operators' compliance with supply chain risk mitigation, and authorize CSE staff to share information with other government entities for the purposes of issuing cybersecurity directions. These new rules and responsibilities risk creating, as I said, a chilling effect, as operators may now hesitate to share information with the cyber centre if they fear it could later be used for regulatory enforcement.

To protect these vital partnerships, we recommend that Bill C-8 better define expected information sharing between CSE and the rest of government and protect information shared voluntarily with the cyber centre from being disclosed. A clear separation between the cyber centre's collaborative functions and CSE's new obligations could be adopted.

We can draw inspiration from a similar model that already exists in our sector between the North American Electric Reliability Corporation, or NERC, and the electricity information-sharing and analysis centre, or the E-ISAC. Although the E-ISAC is operated by NERC, it is kept organizationally isolated from enforcement activities, which preserves confidentiality and encourages open information exchange with electricity operators.

Finally, we're concerned that Bill C-8 could create a duplicative regulatory framework for cybersecurity in the electricity sector, which is already regulated through NERC standards and provincial regulators. The electricity sector is unique in that it adheres to NERC's critical infrastructure protection standards, which are adopted, enforced and audited by provincial bodies. These standards already ensure strong and comprehensive measures to secure the grid. Introducing new, potentially conflicting, federal requirements risks creating ambiguity, additional compliance burdens and regulatory misalignment, all of which could undermine the bill's objective of enhancing security.

To mitigate this risk, we propose including provisions that allow the federal regulator to recognize and accept compliance with equivalent frameworks, such as NERC's CIP. We'll also be ready to work with the government during the regulatory development process to ensure alignment and harmonization with existing frameworks.

[*Translation*]

While there are many other aspects of the bill that also deserve attention, that's all the time I have today—

The Vice-Chair (Claude DeBellefeuille): You took the words right out of my mouth, Mr. Bradley. Your time is up.

We will now begin the first round of questions.

Mr. Lloyd, you have the floor for six minutes.

● (1225)

[*English*]

Dane Lloyd: Thank you to the witnesses.

Thank you, Madam Chair.

Mr. Bradley, is there a precedent for these safe harbour provisions you're proposing in other jurisdictions, and if so, in which jurisdictions?

Francis Bradley: That is an excellent question. I don't have a great deal of detail specifically with the safe harbour—

Dane Lloyd: Can you send that at a later time, then, if you can get a briefing on it?

Francis Bradley: We can.

I would also reference the witness you had previously from the CCTX, who spoke in detail about safe harbour provisions and has provided detail on that.

Dane Lloyd: Okay, thank you.

We want to give protections to the operators so they share information, but what if the case is that the operator was found to be grossly negligent in causing a cybersecurity incident? Would these safe harbour provisions protect them from criminal prosecution when they share that information with the government?

Francis Bradley: If you're talking about a case of clear.... I'm sorry; what was the term you used?

Dane Lloyd: It was gross negligence.

Francis Bradley: I don't believe that would apply when you're talking about safe harbour provisions.

Dane Lloyd: Thank you.

We don't want companies to use the safe harbour provisions to say you can't investigate them or charge them because they shared the information with you.

Francis Bradley: That's correct.

Dane Lloyd: Okay.

Do you agree with other industry stakeholders—we've received a brief from the electronic payments association—that the reporting requirements for all cybersecurity changes are too broad and could lead to a heavy reporting burden on operators without improving security outcomes?

Francis Bradley: We don't exactly know what the reporting burden is going to be, because we haven't seen the regulations. Our concern is about doubling and layering on. We already have an existing mandatory regime. That is unique for the electricity sector because of the NERC standards. We have mandatory reporting already in this sector. Our concern is not so much what that reporting regime is going to be. We already have one.

Dane Lloyd: Is there a legislative change that you think could help reduce this duplicative burden?

Francis Bradley: Yes. Right now, as the legislation is written, the order in council "may" identify equivalent standards. It should be that they "should" be identifying them. As opposed to making it optional, it should be mandatory that existing mandatory standards be regarded as equivalent.

Dane Lloyd: Thank you.

Can you tell us about any concerns pertaining to the administrative monetary penalties proposed in this legislation? Do you believe that monetary penalties are a constructive tool for driving compliance?

Francis Bradley: Monetary penalties already exist for our sector. With respect to CIP, there are monetary penalties in NERC CIP standards. We haven't seen major monetary penalties yet on Canadian entities, but on a North American basis, we have seen six-figure monetary penalties for CIP standards.

Dane Lloyd: Did they help in driving compliance, or were they a hindrance?

Francis Bradley: I don't think they impact compliance.

Dane Lloyd: Do you have any concerns that the mandatory information-sharing provisions in the CCSPA could inadvertently lead to disclosure of sensitive commercial, operational or even personal employee data? If so, do you think the bill should be amended to better safeguard that information?

Francis Bradley: We already exchange very sensitive information on an ongoing basis. The protections that I believe are in place now are likely sufficient. Our concern is not so much the protection of the information, but the potential that information could be used for more than simply improving security. If it's used for penalty, if it's used by the regulator as opposed to the security people, that is where our concern would come in.

Dane Lloyd: Thank you.

The bill also proposes to introduce significant penalties and potential liability for officers and directors of designated entities. We've heard from other stakeholders that there isn't really precedent for this in other jurisdictions.

Do you have any thoughts on those provisions?

Francis Bradley: I do not know about other jurisdictions.

Dane Lloyd: What is it like within Canada?

Francis Bradley: On the one hand, officers of corporations are ultimately those who are responsible for the actions of those entities to begin with.

On the other hand, there's also directors' and officers' liability insurance, which our organization and many others make sure we have.

Dane Lloyd: Do you share the concerns of other industry stakeholders that the criteria with which we define a designated operator are unclear?

Francis Bradley: I have not seen enough detail on that. Those are the sorts of things I think will be clarified when we get to the regulation stage. I don't think I could pass an opinion on that, because the regulations are not in existence yet.

● (1230)

Dane Lloyd: Some people have said they think the legislation is very unclear about who will be a designated operator and that this could capture a great number of small and medium-sized enterprises.

Thank you for your time.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): You still have 50 seconds, Mr. Lloyd.

[*English*]

Dane Lloyd: Oh, I thought you were telling me I was done.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): No, I gave you the one-minute signal.

[*English*]

Dane Lloyd: Mr. Warnell, do you have any comments on any of those questions I asked?

Todd Warnell: The monetary penalties in this legislation are equivalent to the same liability that officers hold for the safety of their workers.

Cybersecurity is not a stand-alone domain. It is about safe operations of your operator, whatever you happen to be. That approach is already in legislation elsewhere. Its equivalency is actually very beneficial to ensuring the importance of cybersecurity as a core operating practice.

Dane Lloyd: Do you think this legislation will help protect our electrical system from the threat of solar flares and coronal events?

Todd Warnell: No, this is definitely not doing anything around enhancing natural protections. There are other works in other areas that could further that.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I apologize for stopping you there, Mr. Warnell. Perhaps you'll have a chance to finish your answer in another round.

I now give the floor to Mr. Ramsay for six minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Thank you, Madam Chair.

I'd like to thank the witnesses for their presentations.

We heard from the previous panel about privacy risks. Whether this is valid remains to be seen, as we heard from a previous panel that the protections in the bill were sufficient. However, I think that it is important to look at the advantages and disadvantages of this bill, as we must do for every bill.

In connection with that, I'd like you to tell us what the dangers are and what the consequences of cyber threats are for your respective industries. How serious could these potential attacks be? What does it mean for the average person?

[*English*]

Francis Bradley: Perhaps I can begin. In terms of what the potential impact for cyber-attacks is, I believe that the sector has been very effective in terms of its cyber protection, but if you want to understand what the potential impacts could be, you'd have to go back to 2015, when we saw, for the first time, electricity service to end customers impacted by the cyber-attack by Russia in Ukraine, which actually turned off the lights for customers.

That is not something we've seen here in Canada. If you want to understand what the worst-case scenario potential risk is, it's loss of service. Of course, electricity is, in our view, the key infrastructure that every other critical infrastructure in the country depends upon. That is one of the reasons we've worked to develop and have been subject to mandatory cybersecurity standards for close to 20 years now through the work we've done with NERC.

We do have protections in place, because the potential impacts would be so severe if a successful cyber-attack took out power to customers.

Todd Warnell: To echo Mr. Bradley's comments, the broadness of the potential action, both disruptive and destructive, that could be before us is actually incredibly terrifying. The ability for threat actors, both nation-state and cybercriminal actors, to infiltrate networks and cause downtime unexpectedly that cascades into the day-to-day lives of Canadians, whether it's for delivery of health services, water or financial services, because electricity is disrupted, is real. These are no longer hypothetical scenarios, when in previous conversations through the evolution of this bill, I think there was lots of understanding that this was fearmongering.

If you go back to the actual releases from our intelligence partners here in Canada and our allied nations, those realities have been declassified. The reality is that threat actors are pre-positioned, in the event of larger-scale kinetic conflicts or other geopolitical challenges that may decide that this type of action is warranted.

We've moved beyond people with tinfoil hats worried about what could happen to, "It's real." Responding to the threat is necessary, and this is a good first step forward on that.

● (1235)

[*Translation*]

Jacques Ramsay: Mr. Bradley, you alluded to a duplication of regulations. In another meeting, it was clearly explained that it was mainly a matter of providing guidelines and regulations, and that there was, in fact, an agreement to avoid an overlap of services.

Now, as for the incidents that should be reported, I understand that there can be quite a lot of them. I understand that we're going to somewhat clarify what needs to be reported and what is not worth reporting.

Near misses and close calls are not covered in the bill. Could even incidents that ultimately did not occur be so serious that reporting them would be warranted? If so, should that be provided for in the bill?

[*English*]

Francis Bradley: I would start off by saying that, with respect to the potential duplication, this would be addressed in the regulatory process. That is what we were told during Bill C-26 as well. It's not that I doubt the officials involved, but until we actually see the regulation.... Frankly, our experience with the development of regulations following legislation has not always been positive. It has not always resulted in the kinds of regulations that we had been expecting, so we continue to have concerns on that side.

With respect to exactly what will be reported, I might defer part of that to my colleague, Mr. Warnell, as he is a CISO, so he's working at the coal face of cybersecurity.

The concept of having to report near misses.... I'm not sure how one would do that. That one is pretty clear in the area of health and safety, for example. However, I'm not sure what a "near miss" means when we're talking about cybersecurity. I don't know how you would interpret or capture that.

Todd Warnell: I'm happy to—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I'm sorry to interrupt you, Mr. Warnell, but Mr. Ramsay's time is up. I can't let you continue your answer, but you may have a chance to finish it in another round.

Thank you, Mr. Ramsay.

It is now my six-minute turn to ask the witnesses questions.

Mr. Bradley, we are concerned about the whole issue of regulations overlapping with NERC standards.

Can you shed some light on NERC's role in Canada's electricity sector and the risks such an overlap could pose? It's important to understand that.

Francis Bradley: Thank you.

[*English*]

I'd be happy to talk a bit about that NERC relationship, because it is critically important.

[*Translation*]

We feel that the government has not really grasped or understood the regulatory reality in our sector.

NERC creates reliability standards. The provinces adopt the standards and apply them.

[*English*]

I've been involved, for decades, with engagement at NERC. It is an organization that is North American in scope, so this is not a case of some organization that is headquartered in the United States telling us what to do. There are two Canadians on the board of trustees at NERC. There are five Canadians on the members' representatives committee of NERC. We are involved in the development of those standards. This is, clearly, something that has been in existence for a couple of decades. It understands and recognizes the kinds of realities we have, and it has regulatory backstop by Canadian regulators. The NERC standards do have backstops by every regulator in all of the provinces that are part of the bulk power system.

[*Translation*]

What happens when there is an overlap? It leads to higher costs and confusion. Fewer resources are allocated to security and more resources are required for us to respond to different levels and types of regulations.

The Vice-Chair (Claude DeBellefeuille): I have a second question.

As my colleague Jacques Ramsay pointed out, we heard from government officials that their goal was not to create regulatory overlap, but that they would work with your sector to make sure that didn't happen.

Does that reassure you? Personally, I'm still a little concerned. Is that really enough, or should amendments to Bill C-8 be considered to mitigate the risk?

● (1240)

Francis Bradley: Thank you for the question. I was asked the same question a year ago, when we were working on Bill C-26.

We don't doubt the good intentions of our federal government colleagues, but there is no legal obligation in the bill to avoid overlap. We want guarantees in the legislation, rather than waiting for regulations.

What might the solutions be? The provision about compatibility with existing regimes could be strengthened. Instead of being a suggestion, it should be an obligation. I think that's pretty clear. Equivalence should also be recognized. For example, compliance with NERC standards for the protection of critical infrastructure should be considered equal.

[*English*]

As I mentioned previously, our experience, when told, "Don't worry, we'll take care of that in the regulation," has not always been a positive one. When there are clear fixes that should be in the legislation itself, then let's put it in the legislation itself.

If we clearly want to say, "Let's recognize equivalency," as opposed to, "That will be an optional thing that can be looked at in the future," and we know that it's the right way to go, it should be a legislative option as opposed to a regulatory option. In my view, this is something that our legislators should be directing, as opposed to leaving it in the hands of officials who will be writing the regs and implementing them.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I have a minute and a half left and I have one last question for you.

Could you send us proposed amendments that would reflect, for example, your desire for better oversight of this whole issue? Could you send them to us? That way, we could familiarize ourselves with them and get a better understanding of the intent you want to see in the bill.

Francis Bradley: Absolutely, we are actively working on that.

[*English*]

That will be something we will provide specific recommendations on in terms of the specific clauses that we think should be amended that would be able to address this.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I still have a bit of time.

You were saying that Bill C-8 poses risks to your partnership with the Canadian Centre for Cyber Security. Could you tell us a bit, in 30 seconds, what the problem is in that regard?

Francis Bradley: That's really an unintended consequence of the bill. In the electricity sector and other critical infrastructure sectors, we benefit from a very co-operative relationship with the Canadian Centre for Cyber Security. What we want is to preserve that relationship.

[*English*]

The short answer is that we have a very, very strong information-sharing relationship now. This will clearly have a chilling effect if there's even the possibility that information that's being shared could wind up in the hands of regulators.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Bradley.

I now give the floor to Ms. Kirkland for five minutes.

No, wait, I misspoke. Mr. Au is next.

[*English*]

Chak Au: Good. Thank you.

I have questions for Mr. Warnell.

You mentioned private-public partnerships. I think this is a really good idea. On cybersecurity issues, there are technical parts and components to do with technology. I always believe that government does not have the most timely information or technological knowledge. This bill gives the power to the minister to tell the industry what to do and what not to do. I don't think that's the best approach. You guys know better. You're on the ground.

What are your comments in response to having to receive directions from the minister on what to do and what not to do? What is your response to that?

● (1245)

Todd Warnell: The structure of the legislation from our perspective is actually adequate, because it is setting up for "speed of response". The minister themselves will not unilaterally act and provide some arbitrary direction to an industry or an industry participant. They will be working hand in hand with private-public entities. They will be working with and taking technical advice from the Canadian centre for cybersecurity. We don't see the arbitrary nature of an individual minister posing a risk.

When a disruptive or destructive action is about to happen, the opportunity to respond with speed is of the utmost importance. The legislation as laid out allows for that speed of response. It doesn't say to ignore technical experts. It doesn't say to move unilaterally. It is set up for speed of response, which, as we know, in the cybersecurity landscape is of the utmost importance to prevent and/or respond to an event that's unfolding.

Chak Au: Very good.

In your presentation, you also mentioned that Bill C-8 is well intended and needed. Why do you believe, or do you believe, that the bill itself would address most of the problems?

Todd Warnell: I'll build off your question from the previous session.

Candidly, this never ends. With regard to the cyber-threat landscape that is evolving, there is no end. With regard to your previous comment to the last panel, this is a first step. There will be next steps. There will be forever steps. This is because the technology, the capabilities and the cyber-threat landscape will continue to evolve. We're talking and dealing with technologies that are currently mass deployed. We know that AI continues to accelerate now. That is really at a level of focus well before this legislation even came into being in its predecessor form, as Bill C-26.

The reason this bill as it's structured is important is that it doesn't lay out specifically the technologies, the approach or the capabilities that are needed to respond. It is purposefully wide and broad, because we know that it will only continue to evolve very rapidly. That ability of the legislation causes consternation and challenge. I know a lot of industry partners and sectors would like very clear lines of delineation and specificity, but that would undermine the ability to adjust to changing threat landscapes, changing capabilities and changing tactics being used around the world.

Chak Au: Again, obviously, we shouldn't play the game of trying to catch up.

If there is one thing you can recommend so that we can be more proactive, so that we can be ahead of the criminals, what would you recommend?

Todd Warnell: Again, I would recommend continuing to embolden those public-private partnerships, which do exist today. Further indoctrinate those as mandatory elements of coordination and collaboration between government and technical authorities, as well as the competent private sector authorities. That would be my single, best recommendation.

Chak Au: That's very good.

My next question is for Mr. Bradley.

I understand that in regulations and also all kinds of reporting procedures.... You have the professional body. You have the professional industry standard that is already set up. This is another layer that the government is trying to put forward.

Do you agree that, if the industry standard is already higher than the required government standard, it would be better to have the government adopt the professional standard or allow the professional standard to prevail, instead of setting another layer? Would you agree to that?

Francis Bradley: I would agree entirely. That's precisely what we would like to see in this case. We're currently operating under—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I'm sorry for interrupting, Mr. Bradley. My job is not easy when I have to interrupt people who are providing answers.

Thank you very much, Mr. Au.

I now give the floor to Ms. Acan for five minutes.

Sima Acan: Thank you, Madam Chair.

[*English*]

Mr. Warnell, I had the privilege to visit Bruce Power this summer. I want to start by thanking you for the very hard work on the electricity sector and for being the global leader in nuclear usage in medicine for both single-use device sterilization as well as a first-of-its-kind isotope production system. That's used for cancer treatment. You're helping hundreds of thousands of patients.

Ontario produces about 30% of its electricity from Bruce Power, and Ontario contributes around 40% of Canada's GDP. Ensuring a reliable energy supply is a key factor in maintaining our country's economic and national security. Given the critical role that Bruce Power plays in Ontario's electrical supply, why is it essential to protect Canada's critical infrastructure from cyber-threats and other malicious actors?

My second question is this: How does Bill C-8 address these risks?

● (1250)

Todd Warnell: I will start off by saying that Bruce Power's having the ability to continue to operate, provide electricity and stay online, given the defence and depth posture and practices that we have related to security, means nothing if our product can't be delivered to Canadians. It means nothing if it can't get to powering devices in telco or in transportation to allow Canadians to move and communicate around the country. Bruce Power is not an island. We are an essential critical asset, but our product needs to be consumed through the use of electricity throughout the industry.

The importance of this legislation is not about actually improving practices, much as Mr. Bradley was saying. The electricity sector writ large has had mature cybersecurity approaches for two decades or more. Fundamentally, the collective system of systems is vulnerable. The frailty exists in the downstream. Moving and bringing the operating floor and requirement for cybersecurity programs and practices and for supplier risk management to a common level is absolutely in the best interests of all Canadians. I'm not here in the interest today of Bruce Power. I'm here in the interest of making sure that the electricity and the isotopes can get to the places that need them, especially in times of crisis or disruption.

Sima Acan: Thank you very much.

Mr. Bradley, do you want to add anything on that?

Francis Bradley: Sure.

The interdependencies are probably the critical question in this. They always have been, at least from our perspective, as the legislation was first being discussed and as it evolved, really, over the past decade. We were involved in some of those early discussions and were in favour of some kind of legislation, given that the electricity sector, at a bulk level, has mandatory critical infrastructure protection and cybersecurity standards.

Our concern has always been the other interdependent pieces of the economy and supply chain that deliver services to end customers. What about transportation? What about telecommunications? What about finance? They're dependent upon us. We're dependent upon them. We know that our house is in order, but we do have questions about the other sectors.

A broad piece of legislation like this gives us the ability to have a greater assurance that the broader critical infrastructure is being protected. We've always been in favour of seeing this move forward, because of those interdependency concerns.

Sima Acan: Thank you very much.

Mr. Warnell, following the recent emergency preparedness exercise simulating a cyber-attack at Bruce Power, how are Canada's critical infrastructure operators currently prepared to respond to cyber-threats, including at Bruce Power, and in what ways does Bill C-8 enhance their capabilities and provide additional tools for resilience?

Todd Warnell: We were very pleased with the first-of-a-kind evolution of an exercise of that scale, called Huron Unity, which we just completed here in mid-November and had previously focused, based on our regulation, on nuclear security or a nuclear safety challenge. We embedded, for the first time ever, an actual digital disruption event into that as well, to ensure that we can continue to learn and advance towards excellence around multi-scale or multi-faceted events.

The reality of Bill C-8 and why that's important, to extend what we did, is that it will make it acceptable and the prevailing practice of all critical infrastructure sectors to view cybersecurity as not just a sidecar. It's no longer a separate domain. It is essential to business continuity and ensuring that we can drive the outcome.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Warnell. I apologize once again for having to stop you when your comments are very interesting.

It's now my turn to have the floor for two and a half minutes.

Mr. Bradley, I felt you were a bit rushed earlier. Could you tell me about the importance of the partnership you have with the Canadian Centre for Cyber Security? It is important to fully understand the implications of Bill C-8 on that partnership.

● (1255)

[*English*]

Francis Bradley: As I mentioned earlier, we have a very deep relationship with the cyber centre and with the officials. We were one of the first sectors the cyber centre began working closely with. Many of my members, both at the CEO and CIO levels, have security clearances and participate in classified briefings and discussions. In fact, even this week, we had a group in town.

By the same token, there was a great deal of information being shared in that classified space about the challenges and some of the events that are taking place within the sector. It has been a very effective information-sharing relationship. It is a model that I know they're looking at for other sectors for effective information sharing.

Fundamentally, my concern about the legislation would be around whether this results in, as I said earlier, that “chilling effect” of this very effective information sharing that has been developed at both the unclassified and classified levels over many years and could be damaged. We've seen a great deal of value for the sector as a result of those conversations, but so has the cyber centre and, really, critical infrastructure as a whole. The more the folks at the cyber centre are able to learn about the challenges within the sector, the more they'll be able to help other sectors as well.

Those information-sharing channels are absolutely critical, and I would be very concerned about anything that would damage something that we've spent a lot of time looking at, developing and building.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): There is a risk that partners would withhold certain information for fear that it would be misused. Is that correct?

[*English*]

Francis Bradley: Absolutely, and that is a concern that we had two decades ago, as NERC was being stood up and we began having mandatory standards as opposed to simply none.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Thank you, Mr. Bradley. Even when it's my turn, I have to interrupt you when my time is up.

I now give the floor to Mr. Caputo for five minutes.

Frank Caputo: Thank you, Madam Chair.

[*English*]

I would like to begin my time by moving a motion that was put on notice. It has been distributed in both official languages, and I hope all members have had a chance to read it. It's simple and straightforward, and hopefully it can pass quickly with the unanimous support of all colleagues. Then we can get back to committee business.

I don't believe I have to read the motion into the record, because it has been distributed. That's all of my commentary at this time.

Thank you.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): You're officially moving the motion that you put on notice, Mr. Caputo, and now you want to discuss it. Is that correct?

[*English*]

Frank Caputo: The motion is essentially not to begin clause-by-clause on Bill C-8 until the minister has appeared.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): That's great. The motion is in order, as it relates to Bill C-8.

Are there any comments about the motion that was circulated by Mr. Caputo? Have all committee members received it in both official languages? Is there any discussion?

Mr. Ramsay, the floor is yours.

Jacques Ramsay: Could Mr. Caputo tell us the reasons for this motion? The minister has already testified on Bill C-8.

[*English*]

Frank Caputo: The minister hasn't come. The minister was invited. We want to see the Minister of Industry.

Thank you.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I would indeed like to clarify that, as far as telecommunications are concerned, the Minister of Industry did not testify on Bill C-8.

I think that answers your question, Mr. Ramsay.

Is there any further discussion?

Ms. Acan, you have the floor.

[*English*]

Sima Acan: I would like to move an amendment to the motion to delete everything after Bill C-8.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Okay, you want to move an amendment to Mr. Caputo's motion. Have you circulated it? Has it been discussed? Do you have the text?

Do you want to read your amendment, Ms. Acan?

[*English*]

Sima Acan: I can read it. After the amendment, it will read as follows: “That the chair be instructed to invite the Minister of Industry to appear in relation to the study of Bill C-8.”

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): An amendment to the motion has been moved.

Are there any comments or questions on Ms. Acan's amendment to Mr. Caputo's motion?

Since I see none, we'll have a recorded vote on the amendment.

The vote has ended in a tie. Therefore, the chair has to rule. I am against the amendment proposed by Ms. Acan.

(Amendment negatived: nays 5; yeas 4)

● (1300)

Claude DeBellefeuille: That brings us back to Mr. Caputo's original motion.

Is there any further discussion? If not, we'll go to a vote.

Would you like to comment, Ms. Acan?

[*English*]

Sima Acan: Yes. I would like to make another amendment to the motion, if that's possible, Madam Chair.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Did I understand correctly that you want to propose another amendment?

[*English*]

Sima Acan: It's a different amendment.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Okay. Go ahead, Ms. Acan.

[*English*]

Sima Acan: I would like to make an amendment to remove everything after Bill C-8, but add the following: “no later than Friday, January 30, 2026.” I want this struck from the motion: “and that a meeting for the consideration of clause-by-clause”, I want to add this: “the meeting following the minister's appearance and that the committee does not proceed to other business until the completion of clause-by-clause.”

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): The amendment has just been moved, but it has not been tabled in both official languages.

Mr. Lloyd, do you want to discuss the amendment?

[*English*]

Dane Lloyd: Yes, I'd like to speak to the amendment.

We're just hearing about it for the first time, and it seems somewhat complex, so I would like to see it in writing.

Does the amendment, if I heard it right, say that clause-by-clause will not start until after January 30? It gives the minister until January 30 to appear before the committee, after which clause-by-clause will begin. I want to clarify that.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): I would like to notify you that we have interpretation services until 1:10 p.m. Then we'll have to give the interpreters a 30-minute break before resuming our work. I wanted to let you know that right now we have seven minutes before we have to break, and then we can move on.

Would you like to comment, Ms. Acan?

[*English*]

Sima Acan: Thank you, Madam Chair.

I would like to read it in its entirety, so that it's clear:

> That the chair be instructed to invite the Minister of Industry to appear in relation to the study of Bill C-8 no later than Friday, January 30, 2026, and that a meeting for the consideration of clause-by-clause be scheduled the meeting following the minister's appearance and that the committee not proceed to other business until the completion of clause-by-clause.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Is that understood by everyone? Is that okay?

Is there any discussion on the amendment?

Mr. Caputo, you have the floor.

[*English*]

Frank Caputo: To be clear, does that mean we will be in a position, as with Bill C-12, where we are here literally until midnight or longer? Is that the implication?

[*Translation*]

Sima Acan: No.

A voice: [*Inaudible—Editor*]

The Vice-Chair (Claude DeBellefeuille): Hold on a minute. Let me remind you that Mr. Caputo is addressing his question to the chair.

Ms. Acan, would you like to answer Mr. Caputo's question?

Sima Acan: The answer is no, Madam Chair.

The Vice-Chair (Claude DeBellefeuille): Mr. Lloyd, do you want to speak?

[*English*]

Dane Lloyd: Thank you, Madam Chair.

Thank you for the clarification from the member opposite.

That is the end of a sitting week. Does that mean there could be no new business prior to that meeting with the industry minister? On the Tuesday, for example, there can't be any new business put forward. Is that correct?

Sima Acan: I believe so. It's just that we would do clause-by-clause every meeting until it's done. That's my intention.

● (1305)

Dane Lloyd: Okay, so—

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Hold on a minute, Mr. Lloyd and Ms. Acan. I will give the floor to the clerk, who can clarify.

[*English*]

The Clerk: Madam Acan, are you trying to make it so that once the committee starts clause-by-clause, it not proceed to any other business, or do you mean once the minister is invited?

Sima Acan: What I'm saying is that the consideration of....

First, I would like to work on Bill C-8 no later than Friday, January 30, and clause-by-clause consideration is going to be scheduled after the minister's appearance. We would not proceed to any other business until the completion of clause-by-clause.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): Are there any questions or clarifications required on the amendment proposed by Ms. Acan?

Frank Caputo: Madam Chair, I would like the amendment in English, please.

[*English*]

I'd like it in writing, please.

[*Translation*]

The Vice-Chair (Claude DeBellefeuille): That's great. In any event, we only have two minutes of interpretation left, so I suggest we suspend the meeting. When we come back, we'll have the amendment in front of us.

● (1305)

_____(Pause)_____

● (1305)

The Vice-Chair (Claude DeBellefeuille): I call the meeting back to order.

Witnesses, thank you on behalf of my colleagues on the committee. You're excused. Thank you so much for your testimony on Bill C-8.

We were debating the amendment.

Mr. Ramsay, would you like to comment?

Jacques Ramsay: I move to adjourn the discussion until the next time.

The Vice-Chair (Claude DeBellefeuille): You're moving to adjourn the debate until next Tuesday. Is that correct?

● (1310)

Jacques Ramsay: Yes.

The Vice-Chair (Claude DeBellefeuille): Is it the will of the committee to resume this discussion on Tuesday?

Some hon. members: Agreed.

The Vice-Chair (Claude DeBellefeuille): That's great. The meeting is adjourned.