HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

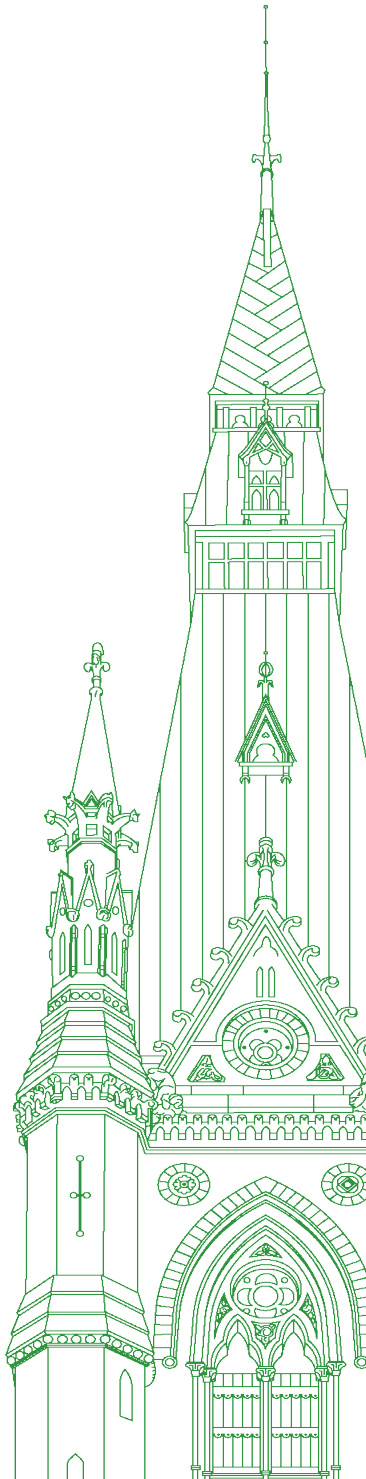
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 039

Thursday, May 28, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Thursday, May 28, 2026

● (1535)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): I call this meeting to order.

Good morning, everyone. Welcome to meeting number 39 of the House of Commons Standing Committee on Public Safety and National Security. Pursuant to the February 26 agenda and Standing Order 81(4), the committee is meeting today as part of its study of main estimates 2026–2027.

I would now like to welcome the Minister of Public Safety and all the many dedicated officials accompanying him today, who I believe will be here for the second hour—which allows us to proceed immediately to the minister's opening remarks for five minutes.

Hon. Gary Anandasangaree (Minister of Public Safety): Mr. Chair, thank you for having me here today to speak about the 2026–27 main estimates for Public Safety Canada portfolios.

[*English*]

I would like to acknowledge that we're meeting on the traditional and unceded territory of the Algonquin Anishinabe people.

I'm joined by my colleagues from their respective portfolio agencies. I want to thank them and their teams for the work they've been doing.

The main estimates reflect our government's priorities to keep communities safe, combat modern national security threats and foreign interference, strengthen our borders and assert our economic sovereignty. We're focused on building stronger, safer communities that are free from violence. That is why, this past March, I announced our renewal of the building safer communities fund. With more than $150 million in funding, we're building on our strong partnerships with municipalities and indigenous communities.

We're supporting the vital work of local community organizations that work day in and day out to provide young people with the opportunities they need to leave a life of crime behind. The results are clear: Young people have the tools they need to succeed, and our communities are better for it. However, this is only one part of our action to cut down on gun violence. We continue to fortify our strategic global partnerships while ensuring that federal policing and public safety institutions remain effective, accountable and financially responsible in a challenging and evolving environment.

On a portfolio-wide basis, the total authorities sought in the main estimates will result in funding approvals of $16.7 billion for the public safety portfolio for the 2026-27 fiscal year.

[*Translation*]

Allow me to point out some highlights.

[*English*]

For Public Safety Canada, a total of $2.2 billion is sought in these estimates, which includes a funding increase for the first nations and Inuit policing program of $38.2 million, along with a $37.8-million increase to the first nations and Inuit policing facilities program. These programs are fundamental to reconciliation and to improving the safety of indigenous communities.

Our government is continuing to invest in culturally responsive, community-led policing services that are designed and governed in partnership with first nations and Inuit communities. Funding supports both self-administered police services and tripartite agreements with a focus on officer recruitment and retention, training, equipment and community trust.

We have a responsibility to focus resources on core public safety outcomes. That's why we're ensuring that spending is targeted where it delivers the greatest impact, particularly in frontline services and high-risk areas.

Canada Border Services Agency estimates include funding to deliver our government's commitment to hire 1,000 new CBSA officers, reinforce Canada's borders, enhance border integrity and support the land border crossing project.

Similarly, the RCMP funding will expand the RCMP's federal policing workforce by 1,000 new dedicated personnel. The total funding sought is $6.3 billion, of which $263.9 million will support additional capacity for the federal mandate and $173.3 million will support contract policing programs.

For the Correctional Service of Canada, the total funding sought is $4 billion, representing a $138-million increase tied mainly to operating expenditures and compensation due to collective agreement increases.

For the Canadian Security Intelligence Service, the total funding sought is $1 billion, which is an increase of $32.7 million over the previous year.

These are all directed at improving the safety of communities across the country and at our borders, and are in lockstep with our global allies. Again, portfolio-wide, these funding increases are offset by comprehensive expenditure review measures to focus and streamline costs, ensuring the responsible and efficient allocation of taxpayer funds.

I look forward to working jointly with the United States and domestic partners to ensure border security and integrity while building our strategic and economic autonomy. We will continue to improve our ability to detect and respond to national security threats, as well as law enforcement's capacity to fight crime and protect communities.

[*Translation*]

I'm proud to strive to fulfill these duties and to work alongside all of you to keep Canadians safe. Thank you.

The Chair: Thank you, Minister.

I will now yield the floor to Mr. Caputo for six minutes.

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

Welcome, Minister.

[*English*]

Thank you to all of the witnesses. Through the chair, I will be directing all of my questions to the Minister of Public Safety.

Thank you for appearing.

Minister, will you extend the study on Bill C-22, yes or no?

Hon. Gary Anandasangaree: The study on Bill C-22 is undertaken by the committee. As you're aware, Mr. Caputo, each committee controls its own agenda.

Frank Caputo: Then let's not—

Hon. Gary Anandasangaree: I would say that it is up to committee members to determine.

Frank Caputo: Will you recommend or advocate for that right here and right now, yes or no? Here's your opportunity. Will you advocate for the committee to extend the study on Bill C-22? It has been a disaster so far, if we're being honest.

Will you extend the study for that reason? Will you advocate for the extension of that study, yes or no?

● (1540)

Hon. Gary Anandasangaree: Mr. Caputo, I will leave it up to committee members to make that determination.

Frank Caputo: You don't think we should be hearing from the National Council of Canadian Muslims. Is that right, Minister?

Hon. Gary Anandasangaree: Mr. Caputo, I don't determine who appears as witnesses. Those are priorities that you set and this committee sets.

Frank Caputo: I don't set them.

Hon. Gary Anandasangaree: I am not about to pre-empt any witness list. That's work for yourselves.

Frank Caputo: Minister, let's not kid ourselves here. Your government has a majority. You can pretty well do whatever you want. Let's be clear: You could give the direction to your parliamentary secretary to ensure that more people are heard from, like Signal and NordVPN.

You won't do that today. You won't advocate for the fact that we should hear from more witnesses. Do I have that right, Minister?

Hon. Gary Anandasangaree: Mr. Caputo, I would also question why any of this is part of the main estimates conversation. I understand that you want to make some additional videos and you're welcome to do that, but let me also say—

Frank Caputo: I have a face for radio, Minister. I'm not making any videos over this one. I'm asking questions on behalf of Canadians. This isn't about videos. This is about a bill that your government—in particular, your department—has rolled out. It has been an unmitigated disaster. It's been a disaster on communications. It's been a disaster on content, and it's been a disaster here in committee. We don't need to talk about making videos. All I'm saying is that you're the minister and the buck stops with you.

Don't you think we should have more time to study this, yes or no?

Hon. Gary Anandasangaree: Mr. Caputo, you will see here that it's the portfolio agencies that are represented, not the members of our government or the chair.

Frank Caputo: Okay. Let's take that as a no.

Hon. Gary Anandasangaree: I would say it is your prerogative as a committee to determine the timelines. That is not on me.

Frank Caputo: Okay. That's a no.

When are you releasing the MOU signed with China on matters of security and intelligence sharing?

Hon. Gary Anandasangaree: Mr. Caputo, we've answered that question a number of times. I will say that as of 2010, we've had a number of very similar agreements that were entered into with China—

Frank Caputo: Was China designated as...? Did we have a foreign interference inquiry in 2010? My timelines must be off here, because things have certainly changed since 2010, Minister, and you and I both know that.

Sam Cooper reported that the reason this isn't being released is that China would have to sign off. Does China need to sign off on this, yes or no?

Hon. Gary Anandasangaree: Mr. Caputo, we are following convention. Since 2010, we have not—

Frank Caputo: I don't care about 2010, Minister. I care about whether China has to sign off.

Hon. Gary Anandasangaree: Mr. Caputo, if you want an answer, you need to give me some time to give you an answer.

Frank Caputo: You are answering questions I'm not asking, Minister.

I'm going to ask you this: Does China have to sign off on this MOU being released? That's it. Just give a yes or a no, please.

Hon. Gary Anandasangaree: The MOU in question is very similar to other MOUs that were signed since 2010, including by previous prime minister Stephen Harper. The convention has been that these documents are typically not released.

Frank Caputo: I'm not asking about conventions, Minister. Please stop answering questions I'm not asking. Does China need to sign off on this MOU being released, yes or no?

Hon. Gary Anandasangaree: This is our convention. This is the practice that we—

Frank Caputo: The convention is for China to have to sign off.

Hon. Gary Anandasangaree: Mr. Caputo, don't put words in my mouth. Let's not trivialize the very important issue that you're undertaking here.

Frank Caputo: Let's not.

Hon. Gary Anandasangaree: Yes, let's not. The MOU with China was entered into a number of times, including in 2010 under previous prime minister Stephen Harper. They have never been made public and that continues to be the convention.

Frank Caputo: Also, there wasn't a foreign interference inquiry. We had members of Parliament who lost their seats because of foreign interference. That happened under your government's watch, Minister, so please don't lecture me about Stephen Harper and how things have changed.

Does that MOU need China's sign-off to get released, yes or no?

Hon. Gary Anandasangaree: As I've said already, that is the prerogative of our government, and as convention dictates, we do not release the MOUs—

Frank Caputo: Sam Cooper got it wrong...?

Hon. Gary Anandasangaree: —whether they're with China or other countries, to the public.

Frank Caputo: Are you saying that Sam Cooper got it wrong and that China doesn't need to sign off on that?

Hon. Gary Anandasangaree: I have neither read his article nor follow him.

Frank Caputo: I didn't ask if you've read it.

What he posted says that there has to be sign-off from Beijing. You have skirted around this. You can dance all you want, Minister. It's just a simple question, so I'm going to frame it simply. Does Beijing need to sign off on this MOU being released, notwithstanding the prerogative and notwithstanding Stephen Harper?

Does Beijing need to sign off, yes or no?

● (1545)

Hon. Gary Anandasangaree: It is our government that needs to sign off, Mr. Caputo.

Frank Caputo: Your government won't be transparent with Canadians. Is that right?

Hon. Gary Anandasangaree: Let's not play games here.

Frank Caputo: I'm not playing games.

Hon. Gary Anandasangaree: Let's get back to—

The Chair: I'm sorry to interrupt both of you, but that's all the time we have for this first intervention.

Let me now move to Ms. Dandurand for six minutes, please.

[*Translation*]

Marianne Dandurand (Compton—Stanstead, Lib.): Thank you very much, Mr. Chair.

Minister, thank you for joining us.

First, I would like to remind my colleague Mr. Caputo that we introduced a motion to hear from more witnesses on the issue he mentioned. Accordingly, we would very much like to move forward with this motion.

Minister, I would like to draw your attention to a topic that is very important to me: cellular connectivity.

I come from a particularly mountainous region and live in a city of nearly 200,000 people. Yet, at home, I have no cell service—and I won't even go into all the rural communities around Sherbrooke. Many of them have no cellular connectivity.

For example, I've had reports from firefighters who have to leave the scene of an emergency to call for backup. Sometimes paramedics have no service either. If you're in a car accident, sometimes you can't reach emergency services. There are also shelters that find themselves in situations where they have no connection.

I would therefore like to know more about the importance the Department of Public Safety places on the issue of cellular connectivity in rural areas and what actions are being taken to improve the situation.

Hon. Gary Anandasangaree: Thank you, Ms. Dandurand.

First of all, thank you for the question. I know that you are at the forefront of this issue and that your work is very important in moving this critical issue forward.

[*English*]

I have to say that I had the pleasure of visiting your community. I met with many civic leaders, including the fire chief. I understood first-hand, I think, the complexity, especially around border towns, not just with respect to rural connectivity but also the confusion as to jurisdiction. While I think border towns have always functioned as good neighbours whether they're on the U.S. side or the Canadian side, it is often confusing, and connectivity is a central issue. I fully recognize the challenges. I want to thank you, and I also want to thank the mayors and fire chiefs I met.

I will say that the work continues. We need to ensure that rural communities are connected. That's part of the work of our secretary of state, who continues to work on ensuring that all parts of Canada are connected, especially in Quebec. We will continue to work together to ensure that emergency services, especially, are well equipped with the resources they need to function in remote rural areas.

[*Translation*]

Marianne Dandurand: Thank you very much.

I think the people back home will be very happy to hear that you are concerned about the situation and that the government is taking action on this matter. Let's hope there will soon be developments.

Along the same lines, as you mentioned, my area is a border region. We know there are overall budget constraints and that, sometimes, public safety resources are first cut from areas outside urban centres. However, there are border crossings in my region—just as there are in my colleague Mrs. DeBellefeuille's region—that are very important.

How can we ensure that these vital services—particularly border security services—are maintained, given the current budgetary constraints at the Department of Public Safety?

[*English*]

Hon. Gary Anandasangaree: I'm going to ask if it's okay to ask President O'Gorman to comment as well.

What I will say is that in terms of our border crossings, they're very much aligned to our U.S. counterparts. In terms of timing, in terms of hours of service, they're aligned, and they mirror what our colleagues on the U.S. side do toward border control.

The unique feature, I think, especially in your community, is that emergency services, for example, sometimes come in from the U.S. side. That can often be frustrating for community members, especially when it's an emergency. We're very sympathetic to that, and we are working towards a solution.

Maybe I can ask Ms. O'Gorman to comment further.

● (1550)

[*Translation*]

Erin O'Gorman (President, Canada Border Services Agency): To reinforce this point, I will say we have agreements with our United States colleagues for emergency services. As the minister said, we are aligning our schedules. It is challenging when one point of entry is open while the other is not. So this work has been very important. We also entered into additional agreements so that, in the event of an emergency, services can be provided on both sides of the border.

I'm not sure if your question included infrastructure, but we've made significant investments in Lacolle, as well as smaller investments at smaller points of entry. We're ensuring we have replacement infrastructure across the country.

The Chair: Unfortunately, that is all the time we have, Ms. Dandurand.

Mrs. DeBellefeuille, you have the floor for six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Thank you very much, Mr. Chair.

Minister, welcome to you and your team.

I am going to speak to you about a subject that is of great concern to you: human trafficking.

I was surprised to find that, according to Statistics Canada data, between 2009 and 2019, Quebec ranked second, and that from 2019 to 2024, Quebec dropped to fourth place. In trying to understand this decrease, I realized that, since 2019, Statistics Canada has been using data from the Canadian Human Trafficking Hotline, in addition to cases reported to the police.

But that is problematic, because you received a report from the Quebec Coalition Against Human Trafficking indicating that francophones in Quebec are not receiving quality, professional service from the Canadian Human Trafficking Hotline. I don't know whether you are aware of this. Did you receive this report?

[*English*]

Hon. Gary Anandasangaree: I have not read the report, but I will say I am familiar with the situation. In fact, when I was in Sherbrooke—

[*Translation*]

Claude DeBellefeuille: Excuse me for interrupting, Minister. I asked if you had received it. You told me you hadn't read it, but that you were aware of the issue. That was your answer.

I'll just summarize what the report says, because it's important for the people following our work. In 90% of cases, when francophones call, an anglophone answers. They are then redirected to a subcontractor. The group you fund to the tune of $12.5 million uses a subcontractor. However, the subcontractor does not understand the Quebec accent, so they direct people to 811, the Info-Santé service.

In my view, the group you are funding to the tune of $12.5 million is not providing an adequate, high-quality and professional service to francophone victims or survivors of human trafficking. Do you intend to investigate this matter and demand that the group take corrective action? That is my first question.

Here is my second question. In my opinion, it would be simpler for you to fund the Quebec Coalition Against Human Trafficking to provide 100% French-language services with professionals who are familiar with the resource network. Currently, the subcontractor responding in French is based in Toronto. They do not understand and are not familiar with the resources.

Will you commit to making significant changes so that Quebec francophones have access to the same service, of the same quality, as that offered to anglophones?

[*English*]

Hon. Gary Anandasangaree: Thank you, Madame DeBellefeuille.

I did have a round table when I was in Sherbrooke, probably in the fall, where we heard from those who were helping survivors and family members on the lack of French language services. It is something that has come to my attention.

I wasn't familiar with this particular issue vis-à-vis the provision of fluency in French. It's something that I will certainly look into, and I will get back to you.

● (1555)

[*Translation*]

Claude DeBellefeuille: I am going to hand you a document written in French. I do want to tell you, however, that last April, coalition members met with representatives from your department, but there was no follow-up.

This is not a trivial matter; it involves human trafficking. As we speak, francophones are being discriminated against and marginalized. It seems to me that with a report and a meeting on April 15, things should have moved forward. It's now the end of May, so I'm quite disappointed—if not angry—about the way your department is treating the Quebec Coalition Against Human Trafficking.

Will you commit to meeting with representatives of the coalition promptly and ensuring its funding so it can offer a human trafficking hotline in Quebec in French and with a Quebec accent?

[*English*]

Hon. Gary Anandasangaree: I'm usually very transparent in these things. I absolutely undertake to do that. I would also look for your assistance as we meet with them, to ensure that the appropriate services are extended.

[*Translation*]

Claude DeBellefeuille: With the time I have left, I'll tell you frankly that the group in question is widely recognized in Quebec for its expertise, and it doesn't understand your department's complacency. It would be much simpler if it were Quebec francophones helping people who are—let's face it—largely in the Montreal area, because the group you're funding uses subcontractors who do speak passable French, but who lack the professional skills or local knowledge to take action. I expect there to be changes, because today, many people are following our work, and we're talking about human trafficking here.

Can I count on a commitment from you and your deputy minister to make a change, and can I hope for funding for the Quebec organization that deals with human trafficking?

[*English*]

Hon. Gary Anandasangaree: I will undertake to look into this and ensure that there's fairness. I'll also undertake to ensure that for the language of choice, particularly French, there are adequate and appropriate levels of French-language fluency in the delivery of these programs.

That's the mandate we have. We certainly have that built into all of our agreements. We will certainly speak to the provider and are more than glad to get back to you on this.

[*Translation*]

The Chair: Thank you very much, Mrs. DeBellefeuille.

Ms. Kirkland, the floor is yours for five minutes.

[*English*]

Rhonda Kirkland (Oshawa, CPC): Thank you, Minister, for being here today. My questions are for you.

Initially, I'll be asking just a few yes-or-no questions as we start out. I promise there are no tricks here.

I think you would agree that public trust is essential when Parliament considers legislation affecting Canadians' privacy and digital communications. Would you agree that public trust is essential?

Hon. Gary Anandasangaree: My role, and especially that of public safety—

Rhonda Kirkland: Is that a yes? Come on. Is it yes or no?

Hon. Gary Anandasangaree: I don't do yes-and-no answers. If I may—

A voice: Oh, oh!

Rhonda Kirkland: I'm sorry. I'm going to stop you for just a second. It's really a simple question.

Is public trust essential when we're making laws in this country that affect people's privacy and digital communications?

Hon. Gary Anandasangaree: Public trust is always important and essential in all of my functions as a minister.

Rhonda Kirkland: Okay. That's perfect—amazing.

Would you also agree that trust can be undermined when Canadians are unclear about how their personal data might be accessed or protected under the law?

Hon. Gary Anandasangaree: Trust certainly can be broken or challenged in a number of circumstances, including when misinformation is out there in social media, when basic issues are misconstrued—

Rhonda Kirkland: Yes, I agree—

Hon. Gary Anandasangaree: —when things that are not in a particular bill, for example, are espoused as being—

Rhonda Kirkland: I'm going to interrupt. I'm sorry. I just want to get back to....

I agree with what you say about things being misrepresented. That's why time is essential. For people to understand something, they need time to process and to absorb.

Do you think that lawful access powers, for instance, as in Bill C-22, must always meet necessity and proportionality standards?

Hon. Gary Anandasangaree: I've spoken about the bill on a number of occasions. I would say that the bill in front of this committee right now certainly attempts to balance—I wouldn't say perfectly—a number of competing interests. Any additional powers and authorities given to law enforcement are punctuated by ensuring that the privacy rights of individuals are protected, and there's actual judicial oversight and authorization. In areas where—

● (1600)

Rhonda Kirkland: I'll stop you there because that answers my question.

Should Canadians have absolute clarity, then, about when and how their private communications can be accessed by the state? They should understand. Is that not correct?

Hon. Gary Anandasangaree: I think parliamentarians need to understand that as well, and that's why we've taken a number of steps.

Rhonda Kirkland: Do you not think that Canadians should have clarity?

Hon. Gary Anandasangaree: I think the first step is for parliamentarians...but, certainly, Canadians also need to have that confidence and trust.

Rhonda Kirkland: I think you would agree that when there is any uncertainty in privacy law, it can be just as damaging as overreach. Is that right? Uncertainty can be just as damaging as overreach because it changes how Canadians behave online. Would you agree with that?

Hon. Gary Anandasangaree: The lawful access bill that's in front of you has found the appropriate balance between the protection of privacy rights and privacy interest. There's a reasonable expectation of privacy for all of us who are engaged with or use electronic devices.

Rhonda Kirkland: You believe.... I'll take that to—

Hon. Gary Anandasangaree: That is a basic principle that we're working with.

Rhonda Kirkland: Let me go back to what you said.

You believe it strikes the proper balance. Yesterday, you criticized big tech companies and suggested they needed to step up in protecting Canadians' privacy rights, and that may be true. You even accused them of misinformation.

Apple, Google, Meta, Signal, civil liberty groups and privacy law experts, including the Privacy Commissioner of Canada, all testified that Bill C-22 could weaken encryption, create systemic vulnerabilities and expose Canadians to greater cybersecurity threats, putting our security even more at risk. Were all of those witnesses wrong, including the Privacy Commissioner?

Hon. Gary Anandasangaree: Ms. Kirkland, let me.... What I've said on encryption is that we will be more than willing to look at amendments that strengthen encryption and that don't, in any way, compromise encryption.

Rhonda Kirkland: This is about more than just encryption, with all due respect.

Hon. Gary Anandasangaree: There are a number of things that you put forward there. With all due respect, it's not helpful for us to argue on points that I've already addressed.

For example, on encryption—

Rhonda Kirkland: I understand this already. I'm just trying to help Canadians understand it, so could you just be careful about how you're responding back to me?

Hon. Gary Anandasangaree: Sure. On encryption, let's talk—

Rhonda Kirkland: It feels a bit like you're trying to....

I've been studying this legislation. I understand it. I don't want to accuse you of sounding a certain way, so we're just going to back up right there for a second. The Privacy Commissioner of Canada testified. He was here. He said that Bill C-22 poses significant privacy risks, and he recommended narrowing the scope of the bill.

Will you commit to doing that?

The Chair: I'm sorry to interrupt what could have been a useful answer, but that's all the time we have for now.

Rhonda Kirkland: You've been saved by the bell.

The Chair: Mr. Powlowski, go ahead for five minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Minister, it's quite apparent that Conservatives like to ask questions, but they're not too interested in the answers. You did talk and you seemed to want to talk about the issue of encryption in Bill C-22. I'll give you the opportunity to actually answer the question.

Hon. Gary Anandasangaree: Thank you, Mr. Powlowski.

I think I've made clear that, from the outset, Bill C-22 did have protection for when systemic vulnerability is at risk. There's certainly an ability for those who need to comply to not comply with it in the name of systemic vulnerability or creating these vulnerabilities that could potentially impact the system's cybersecurity as a whole.

On the issue of encryption, I have made it absolutely clear, and I made a number of interventions yesterday where I made it clear, that we're willing to look at it and have the appropriate language put in place. I hope this is where the committee can work towards finding that right language. We may have a proposal. There may be a proposal from our colleagues on the other side. This is where I think the appropriate discussions need to take place as to what kinds of safeguards need to be put in.

There's no question that the intention was never to jeopardize encryption. The commitment that we have today, which I've made clearly, is that encryption should not be compromised under any circumstances.

● (1605)

Marcus Powlowski: Thank you.

Now I'll ask the questions I want to ask concerning my riding.

I know Commissioner Larkin is here, so maybe this is more of a question for him.

There used to be something like 26 RCMP officers between White River and the Manitoba border. It was down to two, but I believe it's up to three. We've heard a lot about 1,000 new RCMP officers, but I don't think Thunder Bay has yet to see more than one, even though they're trying to increase the numbers beyond that.

Can you give me some idea as to when we can hope to get some new RCMP officers?

Senior Deputy Commissioner Bryan Larkin (Royal Canadian Mounted Police): The RCMP investment from the Government of Canada in the 1,000 is for the federal mandate. You will see those 750 regular members, which are police officers, supported by 250 public servants and/or specialized skills. The design is to deploy them across the country in our four federal policing regions. Clearly, Ontario is its own region: central region. It's a large land mass with significant national security work, supporting our colleagues at the CBSA through border integrity, as well as serious organized crime. Those are rolling out right now, so we anticipate, by the end of the fiscal first year, adding 350 regular members across the country. Those are not centric to national headquarters; those are centric to the regions supporting the federal policing mandate.

I recognize that there is a detachment in Thunder Bay, and that staffing allocation is still an internal discussion as we look at vulnerabilities not only in Ontario but across the country. You will see a large infusion in the range of about 200 additional federal policing regular members in central region. They'll be dispersed throughout the province of Ontario.

Marcus Powlowski: My other understanding is that an impediment to getting officers in that region doing federal policing was the fact that in a lot of places where they have contract policing, like in the Prairies, the officer in charge had to sign off on somebody transferring out of those regions, and they were refusing to allow officers in those places to move to other places.

I think we had the head of the union of the RCMP here who said that was changing. Can you tell me if that has changed, or do we still have the problem or the situation where the officer in charge of groups of police across Canada can veto transfers?

D/Commr Bryan Larkin: What you're speaking about is releasability. Obviously, we manage releasability across our nation to ensure that every province and territory where we may be the provincial or territorial police service is not impacted, and to create public safety in those communities where we provide support for provincial, territorial and municipal policing.

What I can tell you is that the commissioner has issued a federal policing releasability mandate, which directs all commanding officers across the country with set targets so that we can meet the RCMP 1,000 and ensure that the federal policing program is a priority within our organization. Each province and territory does have a signal around its year-one, year-two and year-three targets, because the addition of the 1,000 is over a three-year period. That ensures a balanced, strategic approach to ensuring staffing across our nation without creating any gaps and/or vulnerabilities in any community, which is important. We must ensure that our country is safe and secure, so that's a very delicate balance.

I can tell you that we have a strategic approach around quarterly releasability, and that's tied to a learning curriculum, a recruiting curriculum, which brings a very strategic focus to our organization.

The Chair: Thank you, MP Powlowski.

[*Translation*]

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

Minister, earlier we talked about discrimination between francophones and anglophones in the services provided by a community organization, more specifically the Canadian Human Trafficking Hotline.

I discovered another intolerable situation. The Integrated Threat Assessment Centre, which operates under the Canadian Security Intelligence Service, publishes small pamphlets and publications such as “Threats to Canada Related to the Conflict in the Middle East” fairly regularly in French-language CEGEPs in Quebec. However, the Cégep de Jonquière drew my attention to the fact that it does not receive as many publications in French as it does in English.

The response it received from the centre is, in my view, unacceptable. According to this response, the centre is making a significant effort to translate its materials as quickly as possible. Its assessments are often produced in response to events. To publish effectively, most of the time, it releases them in English and follows up with a French version. It does not send emails for the French versions. Anyone who frequently visits the centre's portal will see the French reports, which are published regularly. The centre invites the CEGEP to let it know if there is a specific report being sought.

Reading this makes me very angry. These publications are meant to inform people about terrorist threats. They are sent to French-language CEGEPs. Three-quarters of the publications are in English, and when they are requested in French, the response is that the news must be disseminated quickly and that translation services are not available—because, essentially, they are written and distributed in English, even to French-language institutions.

How do you respond to that? Personally, I'm appalled by the situation.

● (1610)

[*English*]

Hon. Gary Anandasangaree: Thank you.

I will say that I am a firm believer that Canadians should have material from the Government of Canada that is in the official language of their usage.

I'm not familiar with this particular issue. Again, I will be more than glad to look into it unless Ms. Giles is able to comment.

[*Translation*]

The Chair: Unfortunately, there won't be enough time.

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

[*English*]

Chak Au (Richmond Centre—Marpole, CPC): Minister, I have some questions for you. They are simple questions, and I hope that I can get simple answers.

As my first question, do you realize that shoplifting has become a national crisis?

Hon. Gary Anandasangaree: Certainly when we talk about a national crisis, Mr Au, we have to be careful with the context, so—

Chak Au: Okay. As my second question, do you know the annual losses caused by shoplifting in the country?

Hon. Gary Anandasangaree: I believe it's $6 billion a year, if I'm not mistaken.

Chak Au: The answer is $9.2 billion.

As question number three, do you know how much losses from shoplifting have increased from 2019 to 2025?

Hon. Gary Anandasangaree: No, I'm not familiar with that increase.

Chak Au: They have doubled, from $5 billion to $9.2 billion.

Do you know how much an average grocery store has to spend on preventive measures and security each year?

Hon. Gary Anandasangaree: Mr. Au, I will say that as a government, we are ensuring that the laws are in place to ensure that those—

Chak Au: The answer is $5,000. On average, a grocery store has to spend $5,000 for preventive and security measures.

Do you know the percentage increase in violence in reported shoplifting cases?

Hon. Gary Anandasangaree: Mr. Au, what I will say is that I'm not an expert on shoplifting, but on general issues around public safety, I can speak to what we as a government have been doing to address the issues of public concern.

The concerns that you express are legitimate, and I will say that over the last year we have taken a number of very important steps—

Chak Au: I can give the answer. The increase is 76%.

Do you know the percentage of retailers who feel unsafe in their workplace?

Hon. Gary Anandasangaree: Again, I don't think this is helpful—

Chak Au: The answer is 47%. I will tell you why this is helpful at the end.

Do you know that shoplifting is often related to drug use?

Hon. Gary Anandasangaree: I'm sorry. I didn't understand your....

Chak Au: Do you know that shoplifting is often related to drug use?

Hon. Gary Anandasangaree: It could be, yes.

Chak Au: Okay, that's great.

Do you know that the same offenders are repeatedly arrested and released on the same day?

Hon. Gary Anandasangaree: Again, Mr Au, if you want to speak broadly on public safety, I'm more than glad to give you some commentary as to the steps the government has been taking.

What is not helpful, frankly.... It is like 20 questions to test my knowledge—

Chak Au: I have two more questions.

Amandeep Sodhi (Brampton Centre, Lib.): Mr. Chair, I have a point of order.

With all due respect to my colleague, our minister is here today to answer questions. I don't think it's fair to talk over each other. It's also not healthy for the interpreters doing the interpretation.

Chak Au: Okay. Be patient.

Amandeep Sodhi: Could we give him a chance to answer?

Chak Au: I have two more questions.

The Chair: Thank you, MP Sodhi.

MP Au.

Chak Au: Do you know the percentage of repeat offenders among those arrested for shoplifting?

● (1615)

Hon. Gary Anandasangaree: Mr. Au, I can give you a comprehensive answer in terms of what we, as a government, are doing to address the issues around crime.

Chak Au: The answer is 18%.

My final question is this: Do you have a national strategy to deal with this shoplifting crisis?

Hon. Gary Anandasangaree: I can say that Secretary of State Sahota has been involved in and engaged on this issue. There was a discussion in Peel region very recently. We're certainly open to looking at a national strategy on a range of issues.

I can say that on overall issues around crime, we have Bill C-14, which strengthens bail as well as sentencing. Bill C-16 is on victims' rights. We have Bill C-22, which speaks to lawful access, a tool that law enforcement has been asking for, for many years.

Chak Au: I hope you can come up with an effective strategy to deal with this growing problem. It hurts everybody in the country. When there are losses in monetary terms, it affects affordability, because the loss for the business will just be passed on to the customers. Also, when we have such a large number of retailers telling us that they don't feel safe in their workplace, we should be concerned.

I raised this question four weeks ago in the House. I made a statement. You are telling me that you are not aware of it. Perhaps it was not being paid attention to. I'm just a new MP, so maybe nobody cares about what I say. However, I would be surprised if you're telling me that you are not aware of the problem. I hope this is something you can bring back to your government and work on.

Hon. Gary Anandasangaree: With respect, the way you framed it.... I don't agree with you that it's a national crisis. I think there are a number of issues that take precedence over that in terms of national crises, including the national crisis of missing and murdered indigenous women, girls and two-spirit individuals or the toxic drug crisis.

Certainly, retail theft is an issue. It's something that I'm concerned about, as are all Canadians, but—

The Chair: Minister—

Hon. Gary Anandasangaree: —it doesn't elevate to the level of a national crisis. That's where I started off.

Chak Au: It's organized retail crime.

The Chair: MP Au, I'm sorry to interrupt. We now need to move to MP Housefather for five minutes.

Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chairman.

Mr. Minister, thank you for joining us today.

This weekend on the streets of Montreal, there was a very disturbing rally where politicians were burned in effigy, including one who was visibly Jewish, wearing a kippah. This was roundly denounced by the mayor of Montreal and your Quebec counterpart, as well as you, Mr. Minister.

Can you talk to us about why that type of action is unacceptable in Canadian society and about some of the things the government is doing to deal with the rampant anti-Semitism that has swept this country and the western world?

Hon. Gary Anandasangaree: Thank you, Mr. Housefather, for that question.

Look, I've come to and met with your community a number of times. I've had the opportunity to meet with Jewish communities in many parts of this country, including in Montreal, Ottawa, Toronto, Hamilton, Winnipeg and Vancouver. The level of anti-Semitism is at its height. I wish we were under different circumstances. It is quite worrisome.

We've been working with the law enforcement agencies, including ITAC, to ensure that appropriate updates are done, if required, on the security threat levels. That is essential. At the same time, we are investing in communities. In addition to the $10 million we announced a couple of months ago towards Jewish community security coordination, which is of paramount importance to us, we announced $75 million towards funding over five years for places of gathering. That includes additional dollars towards security guards and so on, which is something the previous program did not allow.

Having said that, Bill C-9 is an important tool that is going through the Senate right now. Again, it responds to some of the current issues being faced, whether it be impeding places of worship or community centres.

This issue is serious. The issue of anti-Semitism is serious. It's hate-motivated. Oftentimes, it's in the backdrop of other world incidents that are taking place. As a government, we absolutely will stand with the Jewish community to ensure their safety and security. This is the resolve of the Prime Minister. This is the resolve of our government, but more work needs to be done. I think all Canadians need to play a part in this as well. When you attack the Jewish community—I've heard this many times—you are not just attacking the Jewish community; you are attacking Canada. You are attacking all communities in Canada. I come from a minority community. I would say that an attack on the Jewish community is an attack on all of us who have come to Canada. My family came as refugees in search of a better place.

This is not acceptable. Our government will do everything it can to ensure the protection of Jewish Canadians, particularly the young people who need to grow up in a society where they can fully actualize their fullest potential.

● (1620)

Anthony Housefather: Thank you.

Thank you so much, Mr. Minister. You've been a tremendous ally in this.

Bill C-9 is the combatting hate act, for those people who don't speak in shorthand. The combatting hate act is a really important tool, but one of the things that need to be done when the combatting hate act gets through the Senate and gets royal assent is that we bring together the provincial public safety ministers, attorneys general and police and get proper training and proper guidance to all police forces across the country as to what is expected of police. I think one of the frustrations has been the feeling that police are not acting on the law.

Mr. Minister, after the law is adopted and royal assent is granted, would you undertake to work with your provincial counterparts to move that forward?

Hon. Gary Anandasangaree: Absolutely. It will be part of the FPT next time around. I do know that Deputy Commissioner Larkin has done a lot of work on this. The RCMP meets with police leaders biweekly, and there is money going toward training as well.

But there is more work to do, and I absolutely undertake to do that work.

Anthony Housefather: Thanks so much.

The Chair: Thank you, MP Housefather.

Next is MP Caputo for five minutes, please.

Frank Caputo: Thank you, Mr. Chair.

Minister, you earlier said that it is the “prerogative” of this government not to release the MOU with China, but you have not once said whether China would have to consent to the MOU being released, regardless of the prerogative.

I'm going to be very clear here. I know you don't like yes-or-no answers, but I think this is one of them: Notwithstanding any of that, does China have to approve the releasing of the MOU—yes or no?

Hon. Gary Anandasangaree: Mr. Caputo, Canada is a sovereign country. We make decisions in the best interests of Canada—

Frank Caputo: I didn't ask that, Minister.

Hon. Gary Anandasangaree: —including disclosure of this said MOU.

Frank Caputo: Minister, I'm not talking about Canada making decisions in its best interests. This is so clear, and you're obfuscating now. Frankly, you and I are both lawyers. I think a judge might find us in contempt if we were obfuscating this way.

Anthony Housefather: On a point of order, Mr. Chair, I know you're not a lawyer, but that is a really serious allegation to say that the minister would be found in contempt by a judge—

Frank Caputo: Fair enough—

Anthony Housefather: I would ask my friend, who's a really good lawyer, to not use that term.

Frank Caputo: Well, we're not getting.... The minister wasn't all that offended. I think the minister takes my point. He would be found to be non-responsive. How about that? The minister would be non-responsive.

Minister, please be responsive. I am not trying to offend you, but I'm trying to drill down on this because this is darn important. You talk about Canada being a sovereign country. I am not talking about that. I am talking about whether China has to approve the release—not Canada, not sovereignty.

Does China have to approve the release, yes or no?

Hon. Gary Anandasangaree: I will repeat that Canada is a sovereign country, Mr. Caputo. We will determine—

Frank Caputo: Minister—

Hon. Gary Anandasangaree: —based on convention, and that's what we have done here, whether to release the MOU or not.

Frank Caputo: What are you trying to hide here? What is the government trying to hide?

You are not coming clean on this, Minister. You're not.

Hon. Gary Anandasangaree: Let me be clear again. I've answered this question a dozen times.

I will say that since 2010 we've had multiple MOUs on security with the Chinese government. They have never been made public, including—

Frank Caputo: When will you be clear, Minister?

Hon. Gary Anandasangaree: —I will say, incidentally, under Prime Minister Harper's leadership.

● (1625)

Frank Caputo: You don't like yes-or-no questions, so I'll say this rhetorically because I won't get a yes or no.

Did Stephen Harper call China our greatest security threat? No, he did not. I'll answer it for you.

Hon. Gary Anandasangaree: Well, I can—

Frank Caputo: Did we have a foreign interference inquiry under Stephen Harper? No. I'll answer that for you.

Transparency demands that this be released. People in the House—let me be clear—people in this chamber potentially lost their seats because of foreign interference. Your Prime Minister, who appointed you and whom you answer to, said that this is the greatest “security threat”, and within less than a year he signs a secret memorandum of understanding with the very nation that he said was the greatest threat to Canada.

Then you come in here, and you won't even tell us—you will not give a clear answer—as to whether they have to sign off. I don't care about Canada.... If it's only about Canada, that's even worse, because then you're not providing the transparency your government has promised.

What is it, Minister?

Hon. Gary Anandasangaree: Mr. Caputo, in the last year, significant world developments—and I don't want to insult your intelligence—have taken place, where Canada needs to expand its trade relations. That is why—

Frank Caputo: Trade...? Trade relations...? This is about intelligence—

Hon. Gary Anandasangaree: May I finish? You had your time.

The Chair: I'm sorry. Please, could we...?

Hon. Gary Anandasangaree: It has to expand its trade relations. We are engaging in relations with a number of countries, including China. Having said that, the Chinese government does not dictate to us which documents are released and which are not. This is within the purview of the Canadian government, so I'm answering your questions very clearly. It is in the purview of a sovereign Canadian government, which has many years, over two decades, of convention, not to release these documents.

To answer your question with a yes or no, no, the Chinese government does not tell us or dictate to us or veto any release of these documents.

Frank Caputo: Okay. It took us four minutes to get there, unfortunately.

Hon. Gary Anandasangaree: These are good clips, though—

Frank Caputo: I'm sorry. Please say it again. Say what you said.

Hon. Gary Anandasangaree: It's all right. Go ahead.

Frank Caputo: No, please, let's hear it.

Let's hear it, Minister. What did you have to say?

Hon. Gary Anandasangaree: You got good clips, Mr. Caputo, so let's continue.

Frank Caputo: No, I'm trying to get answers for Canadians. If you don't want to give them, that's your prerogative.

With that in mind, I will be giving notice of the following motion:

> That, an order of the committee do issue for the government to produce the Memorandum of Understanding on Cooperation in Combating Crimes Between the Royal Canadian Mounted Police and the Ministry of Public Security of the People's Republic of China, signed in January 2026, provided that the document be provided to the clerk of the committee, in an unredacted format and in both official languages, within 10 days of the adoption of this motion.

This isn't about clips. This is about Canadians.

The Chair: Thank you, MP Caputo.

That's a notice of motion that you will certainly share a printed copy of, which will then be translated and shared with other MPs.

That brings us to MP Sodhi for five minutes.

Amandeep Sodhi: Thank you, Mr. Chair.

Thank you to all of our witnesses for being here today.

Minister, there were some questions in the last round that you weren't able to completely answer. Is there an answer of yours that you'd like to complete? I want to give you a bit of time to do that.

Hon. Gary Anandasangaree: Let me address the issues around Bill C-22 and, if I may, take the opportunity to ask Senior Deputy Commissioner Larkin for some comments as well.

Bill C-22 is a very important piece of legislation. I want to acknowledge the co-operation that we've generally had with the opposition, both the Conservatives and the Bloc. I'm grateful that we have had a generally collaborative approach.

What is troubling right now is that, as we move forward on this bill, there is a fair amount of noise. Those concerns that are valid are being addressed, and I do believe, through the committee process, that we will address and strengthen the piece of legislation that's in front of you. It will ensure that we have a lawful access framework that works for law enforcement, and at the same time, we will have a system that protects privacy, extends privacy protections and ensures that there is no back door or illicit way for cybercriminals to have access to that data. We're very clear on that. I do appreciate the work that this committee has been doing.

With your permission, I'll ask the senior deputy commissioner to maybe highlight why Bill C-22 is so important.

D/Commr Bryan Larkin: Thank you, Minister.

It will come as no surprise to this committee that the RCMP and police leaders across the country are very supportive of Bill C-22, as well as the creation of a lawful access regime. We are the only Five Eyes country without a lawful access regime, and when you look at the larger G-20 consortium of countries, we're also the only country that is not a part of that.

For us, this is about victims. For us, this is about solving crime. We believe that there is a balance of opportunities here between public privacy and, quite frankly, allowing lawful investigations. I think that's the key. We're not asking for any unchecked police powers. We're asking for good governance, good democracy and a judicially authorized ability to investigate.

I want to highlight the notion of encryption. Of course, the world has changed. The reality is that we currently do have abilities to intercept and to deal with encryption. However, the reality is that technology is changing at a greater rate than we can keep up with legislative reform.

You've likely heard from some of my colleagues in policing, including Commissioner Carrique, that police leaders and police union executives have been trying to advance a lawful access framework since around 1996. We've come close multiple times. We believe it, in the current geopolitical climate, is a tool that we need. We have significant national security investigations. We have significant serious organized crime investigations where encryption is at the heart of stymying the prosecution and, quite frankly, the undercurrent of solving those crimes.

Again, it will come as no surprise to this committee that the RCMP, along with our policing partners and our colleagues from the service, are supportive of a regime that provides good governance and strong oversight to ensure that there is no unchecked...that puts the privacy of Canadian citizens but doesn't override those who commit the crimes—those individuals who perpetrate crimes against children, perpetrate drug trafficking, perpetrate illicit firearm trafficking.

The tools within Bill C-22 are required for us to be a modernized police community in Canada.

● (1630)

Amandeep Sodhi: Thank you for your answer.

Minister, we heard from Peel Regional Police on Tuesday about the importance of Bill C-22, which you just reiterated, in completing their work.

Yesterday, the Leader of the Opposition stated that Bill C-22 will give the Liberal government sweeping surveillance powers over the information of Canadians. Would you like to comment on this statement?

Hon. Gary Anandasangaree: Sure. It's categorically false, and that's why I think discussion on Bill C-22, especially amongst all of us as parliamentarians, needs to be done in a responsible manner, in a way that doesn't propagate misinformation.

As the senior deputy commissioner said, it's about supporting victims.

Peel Regional Police, in their press conference—and kudos to Chief Nishan Duraiappah, the deputy chief and the whole team—indicated that the arrest could have been made much sooner had a lawful access framework been available. It took a lot of time, especially in cross-border investigation, and involved a number of police jurisdictions. It took a long time for them to get the warrants and the production orders in order to fully investigate before the charges were made. In the meantime, the poor victims in Peel have been struggling with issues of extortion, which is something that I know you're very familiar with and that you've done great work on.

Amandeep Sodhi: Thank you.

The Chair: Thank you, MP Sodhi. That's all the time we have.

[*Translation*]

Minister, thank you for being here and for all the time your team spent preparing for this. Enjoy the rest of your day.

We'll suspend for a few moments.

● (1630)

_____(Pause)_____

● (1635)

● (1640)

The Chair: We are resuming the meeting.

I want to welcome everyone back for the second hour of our committee meeting. I call the meeting back to order.

A number of senior officials are with us. I'll introduce them quickly.

From the Canada Border Services Agency, we welcome Aaron McCrorie, vice-president, intelligence and enforcement; and Ryan Pilgrim, vice-president and chief financial officer. From the Canadian Security Intelligence Service, we welcome Nicole Giles, deputy director, policy, and Jérome Laliberté, deputy director, administration. From the Correctional Service of Canada, we welcome Jay Pike, assistant commissioner, correctional operations and programs sector. From the Department of Public Safety and Emergency Preparedness, we welcome Karine Paré, assistant deputy minister and chief financial officer, and John McKinley, comptroller and deputy chief financial officer. From the Parole Board of Canada, we welcome Claudine Legault, chief financial officer. From the Royal Canadian Mounted Police, we welcome Bryan Larkin, senior deputy commissioner, and Samantha Hazen, chief financial officer.

We'll move straight to questions from members.

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

[*English*]

Frank Caputo: Thank you very much, Mr. Chair.

Deputy Commissioner Larkin, my staff just sent me something here, so I do have to ask you about this. This is from a Global story posted May 21, 2026.

You were here for the minister's remarks, Deputy Commissioner, so you heard him when he said that the release of the MOU was the sole prerogative of the government. Now I'm reading a Global story by Sean Boynton from May 21, 2026. I haven't even read to the end of it yet. This is what it says in the first paragraph:

> The RCMP says it won't release the full agreement it signed with China's Ministry of Public Security without Beijing agreeing to do so, despite demands from the federal Conservatives and NDP for answers on what it contains.

That was seven days ago. I know I'm putting you in a very difficult position here, Deputy Commissioner, in asking you about the RCMP's position on this. If we need to suspend for a few seconds so you can read the story, I'm happy to do that, as long as we extend because this is pretty important. We just had the minister tell us it's the government's prerogative, and it has nothing to do with China.

The story goes on to say:

> "The RCMP will not unilaterally make public or share the contents of an MOU with a third party without the concurrence of the other party," Percival said.
>
> "As such, the RCMP is not releasing the contents of the MOU at this time."

Clearly the RCMP's viewpoint is that it needs the agreement of a third party.

This is what the story says:

> The statement added that such agreements are “a very common practice between national law enforcement agencies” seeking new or enhanced co-operation, and the RCMP has many MOUs in place with agencies around the world.

Then it goes on to say:

> While the full text of many of those MOUs that were signed with China has been released, the one with China's Ministry of Public Security has not.

I wish I had seen this before, when we could have asked the minister about it.

I understand that you're probably in a terribly difficult position because you haven't seen this. Are you able to comment on this at all, Deputy Commissioner?

● (1645)

D/Commr Bryan Larkin: Thank you for the question. I can certainly speak to it from an RCMP perspective.

As this committee and you will be aware, Mr. Caputo, I have significant knowledge of that MOU and I'm happy to provide a larger context around the purpose and how the RCMP engages in MOUs with many different law enforcement agencies across the country.

It would be our organizational position, out of respect for our partnership with the Ministry of Public Security in China and with our partners, and in the approach to good collaboration and good work with another law enforcement agency, that it's generally not the RCMP's position to release MOUs without third party consent.

That said, the RCMP commissioner can, at the direction of the Minister of Public Safety, be directed to release MOUs, etc., in the purview of the government.

Our perspective on that article, although we're not likely to have seen that article but are obviously familiar with the media response and the response of many different journalists, is that the RCMP commissioner and I, as his delegate, would not have the authority and/or the ability to release it without consulting with our partners from the Ministry of Public Security in China.

Again, obviously we take ministerial direction, and that would be within the purview of the Government of Canada, but specifically for the RCMP commissioner, it would be our position that third party consent is appropriate.

Frank Caputo: Thank you. I have your point. Again, I put you on the spot with a tough question, so I appreciate you giving something very quickly.

Is there anything classified in the MOU? Is there anything intelligence-related in the MOU?

D/Commr Bryan Larkin: This is the renewal of an agreement, as the committee is aware. It really opens the door for collaboration. It's not legally binding. There are no enforceable conditions in it. It doesn't compel information sharing. It doesn't override any of our Canadian laws or policing approaches. It creates an opportunity around information sharing, particularly around precursors and fentanyl investigations, and how those investigations are conducted.

In short, in my opinion, there's nothing classified in there. It's a very standard memorandum of understanding, which we have with many different countries as we roll through. It's certainly one that creates the ability for the RCMP to work with a law enforcement agency on how we conduct mutual investigations and how we conduct information sharing. Those are the general thematics.

It also covers—

Frank Caputo: I'm sorry. I'm nearly out of time.

I'll leave you with this rhetorically. I don't understand why we would not release something that is as commonplace as this. You just described it as bland. Why would the government not release it?

I know you can't answer that, but this really [*Technical difficulty—Editor*].

The Chair: [*Technical difficulty—Editor*]

[*Translation*]

Jacques Ramsay (La Prairie—Atateken, Lib.): [*Technical difficulty—Editor*]

● (1705)

The Chair: I apologize for this interruption, everyone. We had to reboot the audio system and ensure that the interpreters are prepared to assist us again.

We were at the beginning of your time, Mr. Ramsay. Could you please start over? You have the floor for six minutes.

Jacques Ramsay: I have some questions for Mr. Pyke first, Ms. Legault, and then I'll come back to you. That will make more sense.

Mr. Pyke, during my visits to correctional facilities, I met many correctional program officers and probation officers. They're worried.

I would like to hear your comments on whether next year's budget will include more or less funding for, first, correctional programs, and second, probation officers, so they can do their jobs.

[*English*]

Jay Pyke (Assistant Commissioner, Correctional Operations and Programs Sector, Correctional Service of Canada): Thank you for your question.

We always have funding—I'm not being facetious—associated with programming and interventions across all sites. In terms of dedicated resource indicators, we have resource indicators based on the ratio of program officers to the offender population, and for correctional program officers, we have the same thing.

There is discussion, obviously, through the comprehensive expenditure review. In looking at the structure of correctional programming and parole overall, there will be some reductions to correctional program officers' positions that will coincide with a new model. We've had preliminary discussions with the union to this point on what that new model will look like.

Moving forward, there will be some reductions to the number of correctional program officers. There will be more support to take care of a lot of the administrative pieces that some of the correctional program officers are seized with right now. It's to allow them to do the actual work of delivering programs. We have had those discussions to this point with USJE, the union representing those members.

● (1710)

[*Translation*]

Jacques Ramsay: Well, I encourage you to do so, because, indeed, one of the complaints we often hear has to do with the increase in paperwork and the time spent drafting documents. If there were a way to reduce the time spent on administrative tasks, I think probation officers could do more of the work expected of them.

Ms. Legault, I'll turn back to you. I was saying that, when there is a parole decision, our colleagues across the floor often accuse the government of being behind that decision. I would like to hear your comments again so you can make it clear to our colleagues that the Parole Board of Canada is independent and impartial.

I would also like you to tell us whether the current budget will allow you to sustain the quality of your work—which I commend, by the way. Finally, I would like to know if your commissioners have identified any gaps in the assistance provided by probation officers to inform the board's work.

Claudine Legault (Chief Financial Officer, Parole Board of Canada): Thank you for the questions.

In terms of the funding allocated to officers, the budget we provide is to ensure that services are delivered and commissioners can render decisions. So, we protect their mandate in this way. The commissioners do indeed make independent decisions, so it is quasi-judicial. Everything related to an inmate is truly independent.

The main estimates specifically ensure the protection of their mandate. In the coming years, we will face constraints due to budget cuts. However, we are effectively ensuring that there are sufficient funds for decision-makers.

As to the relationship between probation officers and commissioners, personally, I am not aware of any complaints that may have been filed. I could relay your question and provide you with that information at a later date.

Jacques Ramsay: All right. I would appreciate that. Mainly, I'm interested in whether there's a general issue, since we're not talking about specific or individual cases, and whether the board members feel they can do their job fully.

Ms. Giles, we know that the types of threats facing Canada are on the rise, as are the intensity and frequency of those threats. I'd like to know whether you plan to review how you've allocated your funding for the next year. If so, can you tell us a little about how you determine the appropriate way of doing that?

Nicole Giles (Deputy Director, Policy, Canadian Security Intelligence Service): Thank you. That's a very good question.

To provide a more specific answer, I'm going to answer in English.

[*English*]

The increasing threats are materializing in terms of the increase in the volume, variety and velocity of the threats. That means we're having to combat and address a whole series of threats, both traditional ones when it comes to espionage or sabotage or foreign interference, and also new ones in terms of the types of ideologically motivated violent extremism we're seeing.

The other challenge we're facing is that technological advances are leading to the threats manifesting much faster than they previously did. This means the threat can move from idea to action much more rapidly, from somebody sitting at a keyboard moving from their ideation of the threat to their actual attempt to perpetrate the threat.

Where that leaves us, as Canada's Security Intelligence Service, is that based on the funding we receive, we are constantly reprioritizing to address the most urgent and serious threats facing Canada. We're regularly reallocating according to the threat environment. We're regularly reallocating in accordance with the work we're doing with our domestic and international partners. The reality is that we require more intelligence and more security intelligence than ever before, but we are sure that Canadians can expect that we will continue to protect them to the very best of our ability.

● (1715)

[*Translation*]

Jacques Ramsay: Thank you.

I have one last question, and it's for you, Mr. McCrorie.

Mr. Larkin, the deputy commissioner, told us that the RCMP was indeed on track to hire the 1,000 personnel in the next three years. I'd like to hear where the CBSA stands on its goal. Are you just as confident that you'll be able to hire the 1,000 CBSA personnel?

Aaron McCrorie (Vice-President, Intelligence and Enforcement, Canada Border Services Agency): Thank you for your question.

[*English*]

I too will answer in English because we're going to use numbers and it'll be better for me to say them in English.

Yes, I think we're on track—

The Chair: I'm sorry. I was confused: I thought the time on my clock was decreasing, but it was increasing. I apologize for interrupting you rudely, but that's well over the time allocated for MP Ramsey.

[*Translation*]

Mrs. DeBellefeuille, you may go ahead for six minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Ms. Giles, can you tell me whether the integrated threat assessment centre is a specialized organization that falls under the administrative oversight of the Canadian Security Intelligence Service, CSIS, and thus under the responsibility of the public safety department? Yes or no?

Nicole Giles: Thank you for your question. I just want to be sure I understand correctly. Are you asking about the integrated threat assessment centre?

Claude DeBellefeuille: Yes. Do you oversee the centre?

Nicole Giles: I, personally, don't oversee the centre, but the director of CSIS does.

Claude DeBellefeuille: Is respecting the Official Languages Act important to CSIS?

Nicole Giles: Yes, of course.

Claude DeBellefeuille: In the first hour, I spoke to the minister about the fact that francophone CEGEPs in Quebec, among others, receive the centre's assessment reports on threats in Canada on a fairly regular basis. The reports provide the people at the CEGEPs with real-time threat information, so they have that awareness. The reports come out fairly regularly.

I told the minister how angry I was when I saw the response that had come from an employee of the centre. According to the employee, unfortunately the centre didn't have the resources to send out English and French alerts and reports simultaneously, but those interested could consult the centre's website, where the reports would eventually be available.

Do you think that response, showing that anglophones and francophones are treated differently, respects your mandate of protecting Quebeckers and Canadians?

Nicole Giles: It is very important to CSIS to communicate in both of Canada's official languages.

[*English*]

It's also important that we communicate with all Canadians, to the extent we can, in the language of their choice, which is why we also translate documents into other languages used in Canada, including some indigenous languages.

Under the Official Languages Act, our employees are able to write in the language of their choice. They will write their assessments in English. They will sometimes write their assessments in French. I would guess that the majority are in English.

[*Translation*]

Claude DeBellefeuille: Respectfully, I'm going to stop you there.

What we are talking about here is a publication that was sent to CEGEPs in Quebec, specifically, the one in Jonquière. The communication that was sent to the CEGEP contained one document in French and four or five documents in English. The institution wondered what was going on and why the communication didn't include the same number of documents in French. The centre's response was that it couldn't provide the French documents at the same time, because it didn't have the capacity to do so in real time.

That response is unacceptable. Your job is to protect francophones, anglophones and everyone living in Canada. Right now, however, you're providing better information and more information to anglophones.

With all the translation options out there, that is unacceptable. The translation bureau is busy. I get it, but CSIS has the ability to get it done, especially since your job is to protect people and that hinges on the information you give them.

I wasn't a police officer. I was a social worker and a manager in the public health system, but I know enough to know that when you don't get the information you need in an emergency in the language you need it in, your ability to take the appropriate precautions is hindered.

Everyone is aware of the problem now. What I want to know is what you're going to do to fix it. How are you going to make sure that, from now on, educational institutions and all other French-speaking partners have access to the same quantity and quality of information from the centre? What are you going to do?

● (1720)

Nicole Giles: I completely agree that it's very important to make sure that information regarding threats is provided to all Canadians in the language of their choice. I fully agree with that.

[*English*]

I'm not aware of the particular issue or correspondence. My firm commitment to the committee is that I will take that information and look into it, and we will do whatever we can to ensure that the language of choice is respected when we're sending out documents.

Unfortunately, I'm not aware of the particular correspondence in this particular case, but CSIS's commitment is to ensure that we follow the Official Languages Act, and wherever possible, we are putting out material in both official languages.

[*Translation*]

Claude DeBellefeuille: I'm glad to hear you make that commitment, but it's going to require an organizational change. This isn't something that allegedly happened; it's a fact, and it's been this way for a while. What it tells me is that CSIS cares less about keeping francophones safe from terrorist threats, because it doesn't have the capacity to give them the information they need.

Starting now, I expect you to make major changes to ensure that your French-speaking partners receive the same quantity and quality of information on terrorist threats in Canada as anglophones do. Do you commit to doing that?

Nicole Giles: I completely agree. It is very important that information related to threats be provided to our French-speaking partners. It is essential that all Canadians receive equal protection. That is a very firm commitment on the part of CSIS. What I'm going to do is take note of the situation, ask questions internally and investigate to make sure the information is being provided in both official languages.

The Chair: Thank you, Mrs. DeBellefeuille.

Ms. Kronis, you may go ahead. You have five minutes.

[*English*]

However, I'll give you one more minute, given that I was a bit too generous to the previous Liberal speaker.

[*Translation*]

Tamara Kronis (Nanaimo—Ladysmith, CPC): Thank you, Mr. Chair.

[*English*]

My questions will be for Ms. Giles as well.

Most Canadians are familiar, at this point, with foreign interference in our elections. I sit on the human rights subcommittee of the foreign affairs committee. We've been studying transnational repression, whereby, as you know, foreign governments target people—often from their own diaspora communities, but sometimes Canadians who support those diaspora communities and others—both online and in other places.

You were talking about the additional threats we are facing in terms of volume, nature and velocity, and you also talked a lot about the technical implications. I want to apply that to our discussions on Bill C-22. Issues around end-to-end encryption have come to this committee in relation to the bill, and I'd like to get your thoughts on this. Is it fair to say that Canadians who are the subjects of transnational repression in Canada are very dependent on communication mechanisms that have strong end-to-end encryption?

Nicole Giles: I think that's a really important question. When it comes to religious, cultural and ethnic communities in Canada that have strong roots in other countries around the world, a number of means of communication are used. The reality is that so many of the publicly available email systems and messaging systems that are used do have encryption built into them. I think from there, it's fair to assume that most Canadians and people in Canada do rely upon different forms of communication, which may or may not have encryption.

● (1725)

Tamara Kronis: Is it fair to say that those who are being targeted by foreign regimes would face, in some cases, serious personal danger if some of the secure mechanisms that they depend on are compromised?

Nicole Giles: I think that when it comes to the threats that individuals are facing in Canada, they can come through a variety of mechanisms. When it comes to foreign interference being perpetrated in Canada, if there are foreign states trying to interfere in a deceptive or covert way with the communications of Canadians and to use that information to bring them harm, it is certainly something that would be a priority for CSIS to examine and to ensure that we're able to work with our domestic partners to combat it.

Tamara Kronis: As we know, these are not hypothetical threats. There have literally been murders in the last year that have been linked to this kind of foreign interference and transnational repression.

What I'm wondering is whether the government has conducted any threat assessments specifically examining how lawful access capability requirements could affect communities vulnerable to transnational repression and those who CSIS is helping in this regard?

Nicole Giles: I think that's, again, a really excellent observation and an excellent question.

What we have done in our examination of the work on Bill C-22 is to try to understand where it is that there are gaps in our lawful access system and where plugging those gaps and bringing our lawful access framework up to the standards of our allies, including European allies and Five Eyes allies, would allow us to better protect Canadians, including from transnational repression.

We believe that having a lawful access regime will better enable us to protect victims of foreign interference and transnational repression in Canada, as well as a number of other threats.

Tamara Kronis: Sometimes when we're trying to help people, we inadvertently have unintended consequences of that. I'm asking about the other implications of it and whether or not the assessments included the possibility that weakened encryption standards or the requirement to have back doors could be exploited by foreign actors looking to do Canadians harm.

Nicole Giles: I can be very clear that there is no expectation and no requirement certainly for back doors to be put in place through Bill C-22. There are not to be any systemic vulnerabilities that are introduced as part of part 2 of Bill C-22. If service providers are concerned about those systemic vulnerabilities, they are able to avail themselves of a number of various steps, including up to judicial review, to challenge that.

Tamara Kronis: With all due respect, judicial review is too late when somebody's come up to your doorstep and put a bullet through your front door.

The issue that I'm asking about is this. We've had a number of experts at this committee who have made it clear that despite the intentions of this bill, there is the reality that encryption could be weakened. The minister himself has indicated that he is willing to accept amendments on this to get it right.

I'm asking you this from a safety and security perspective: Is it important that we get it right?

Nicole Giles: From CSIS's perspective, it's always important that the legislation that's put in place is there to protect Canadians. The parliamentary process always involves quite a bit of back and forth as Parliament works in the best interests of Canadians to ensure that we have the best possible legislation.

I think the minister has expressed his interest in amendments, and we'll certainly support that.

Tamara Kronis: If we get this wrong.... The question I'm asking you is not about whether or not you believe we've struck the right balance. The question is about if we get this wrong.

In the context of the velocity, the volume and the nature, and the changing technology that's out there, is it important to get this right to make sure that people's lives are not at risk?

Nicole Giles: It's always important to ensure that we get the legislation right, and having a proper lawful access regime in place will ensure that we can better protect Canadians.

● (1730)

The Chair: Thank you very much for this intervention.

[*Translation*]

Over to you, Ms. Dandurand, for five minutes.

Marianne Dandurand: Thank you, Mr. Chair.

Thank you all for being here.

You'll notice that I regularly talk about issues that affect people outside large urban centres, because we need resources in the regions as well. I'm going to talk about places like Sherbrooke, which have a lot of halfway houses for people on parole.

Mr. Pyke, I'd like to know whether you have enough resources to support people out on parole in medium-sized cities. How do you support those municipalities, which become somewhat responsible for these people in the community?

[*English*]

Jay Pyke: In terms of capacity, increasing our CBRF—our halfway house or community partner—capacity....

I'm sorry, you lost me with the youth piece because I don't deal with youth. I understand that you mean the succession of youth into our facilities. Is that right?

Marianne Dandurand: It was probably lost in translation. I was asking about regions. How can we help municipalities that have transition centres?

I don't know if it's the right term in English.

[*Translation*]

Jay Pyke: Yes, it's fine. I understand what you mean. Sorry.

[*English*]

Marianne Dandurand: Do we have the resources to help municipalities that receive those people? Those people need help, obviously. How do we help municipalities with those situations?

[*Translation*]

Jay Pyke: Thank you for clarifying, Ms. Dandurand.

[*English*]

We work collectively. Halfway house associations exist across each province, region and district. We will work with our community partners in terms of looking at expansion options. Some may put forward project suggestions for capacity or to increase capacity or programming. We'll work in collaboration with those partners in the community to try to increase that capacity to meet the demands of what we have coming out.

In fact, we have done this across the country. I come from a region myself—a couple of regions, to be candid—and it's always a challenge. A lot of it is balancing expectations with what we have. The other dynamic, particularly in community, is its ability to expand capacity as well. As we know, putting these facilities in the community area is not always popular, so there's lots of engagement with the community and local police to be able to expand.

I can openly say, with an increasing offender population, we are seeing increasing pressure in terms of community bed space and community programming. Funding at this point is not a concern for the CSC in relation to our programs and maintaining a safe reintegration to full extent, but we are always working with community partners in terms of how we expand.

It depends on the region as well, or the area of the region. Obviously, in built-up urban areas, we have a big demand. It's equally challenging in some of the smaller localities depending on the the specifics of the case. We're certainly working on specialized beds in relation to substance use and continuing that care into the community from that. It's the same with aging. We have an aging offender population. I know you were speaking of youth coming through the system, but the reality of it is that we have to match specialized beds inside with specialized community support outside. That's a focus of ours as well.

[*Translation*]

Marianne Dandurand: Thank you.

Switching topics, I want to talk about border security.

Mr. McCrorie, the threats at the border are increasingly complex, ranging from drug trafficking and guns to vehicles and human smuggling. It's important to have strong co-operation with our international partners, especially our American partners in the case of my region, which is near the U.S. border.

How does the funding in the main estimates help you improve your ability to intercept threats at the border?

Aaron McCrorie: Thank you for your question.

[*English*]

Yes, the threats and challenges are constantly evolving. How we try to allocate our resources is based on risk. Where that risk is emerging or where it's changing, we will reallocate our resources accordingly.

The main estimates are providing funding for us to continue that work. They also include the funding for the 1,000 officers. In particular, the 1,000 officers are going to be allocated in areas where we've identified threats and risks that need to be addressed, primarily in terms of our uniformed staff at the border, but also inland. We'll have people working on removals or inland investigation as well as having people doing security screening.

● (1735)

[*Translation*]

Marianne Dandurand: How does it work—

The Chair: Unfortunately, your time is up.

Marianne Dandurand: Thank you.

The Chair: Now we go to Mrs. DeBellefeuille for two and a half minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Mr. Larkin and Ms. Hazen, yesterday in Parliament, our committee chair, whom we are quite fond of, presented the report on our first study. It's on border management. I'm not sure whether you had a chance to look at it, but it contains a series of recommendations. Two of them are especially important to me, so I'd like to know what you think.

First, like Ms. Dandurand, I represent a riding that borders the U.S. My riding is home to an RCMP detachment that works very well with area partners: police forces, and municipal, provincial and federal officials. At the end of the budget cycle, the detachment members set up a satellite post for interviews and storage of rapid response equipment such as snowmobiles and quads. In its report, the committee recommends that the satellite posts be established permanently.

The second recommendation I was talking about has to do with the fact that, when migrants cross the border illegally, small municipalities provide emergency services at the request of the RCMP. That's an additional expense for small municipalities. In our report, we recommend that the RCMP set aside funding to reimburse municipalities for the help they provide in those situations.

Those two recommendations are specifically for the RCMP and would affect its funding. I know you're in the midst of your budget cycle. Can you tell me whether you're supportive of the recommendations? Do you think they're appropriate and would ensure that Canada's borders continued to be managed and controlled properly?

You have 45 seconds left to answer.

[*English*]

Samantha Hazen (Chief Financial Officer, Royal Canadian Mounted Police): Thank you very much for the question.

Through you, Mr. Chair, the RCMP was very grateful to be the recipient of funding to help secure our borders, as part of the fall economic statement in 2024. A $1.3-billion border security package was provided to the entire portfolio.

[*Translation*]

Claude DeBellefeuille: I'm talking about satellite posts in rural communities along the border, mainly Valleyfield, but I know there are others. Does your budget cycle include funding for that?

[*English*]

Samantha Hazen: As part of the onboarding of the 1,000 new personnel for the RCMP, the majority of that personnel will be located outside of the national capital region.

[*Translation*]

Claude DeBellefeuille: That doesn't answer my question at all. I'm talking about satellite posts, not personnel.

[*English*]

Samantha Hazen: All I could share is that there will be an increase in RCMP resources to support our federal mandate, including those to support our border protection. We anticipate that there will be just under 200 more personnel located in the eastern region, which encompasses the province of Quebec and the maritime provinces.

[*Translation*]

The Chair: Thank you.

To make things a bit fairer vis-à-vis the other two parties, I gave you a bit more time, Mrs. DeBellefeuille.

We now go to Mr. Au for five minutes.

[*English*]

Chak Au: I have questions for Mr. Larkin.

Earlier on, when we talked about the MOU between China and Canada on policing co-operation, you mentioned three things. Number one, you said that it's general; number two, you said that this is similar to the previous MOUs; and number three, you mentioned addressing the fentanyl crisis. I find that to be very interesting because, from experience, we know that in the past years the previous MOU has not been effective in stopping the influx of fentanyl into Canada.

If that's the case, why would we again sign an ineffective MOU and expect that it will bring a different result?

D/Commr Bryan Larkin: I'll focus on a couple of broad comments around this.

The RCMP was interested in continuing to renew the MOU around ongoing transnational threats, which include, obviously, drug trafficking—the importation of fentanyl—which we work very closely with our CBSA partners on, threats of foreign actor interference, criminal activity and serious organized crime. These threats, quite frankly, require the RCMP to engage with other law enforcement agencies globally, including the Ministry of Public Security in China. We do have officers located across the Indo-Pacific, liaison officers who work with all agencies.

Again, the engagement and/or participation in these memoranda of understanding should not be mistaken for any endorsement of other countries' conduct. I think that's really important. The reality, though, is that we have a responsibility, as a police agency, to work with all partners. That at times includes countries where we may not, in fact, endorse and/or support the way they operate. However, we have a responsibility. Obviously, we have Canadians who travel, Canadians who go through those countries, including the People's Republic of China. The MOU was designed to re-engage dialogue because it had been stagnant for some time. Our relationship had, quite frankly, been quiet. There had not been much engagement between our organization and the Ministry of Public Security, and it was an opportunity to once again engage in ongoing dialogue, renew that dialogue and look at opportunities.

Again, I would concur that the addiction and fentanyl challenges in our country remain at the forefront, and we're doing significant work with all police services to conduct large-scale investigations.

● (1740)

Chak Au: You mentioned a few more areas in addition to fentanyl. You mentioned foreign interference and other kinds of security concerns.

Do you agree that, judging from past experience, the MOU has not been effective? You also used the word “dialogue”. Are you saying that these MOUs are serving a purpose only on engagement and dialogue, and that there's nothing in the MOU or in the co-operation that could actually be effective in helping our country to become safer?

D/Commr Bryan Larkin: Do we have a matrix that measures the success of the MOU? No, we don't have a matrix. That being said, we've simply.... This one was renewed recently. The commissioner has engaged in dialogue at the United Nations Police Week in New York City with leaders from the Ministry of Public Security, and he intends to do so in the coming months again to reopen doors around some of the challenges we're facing. We do work very closely. We track, for example, precursors that come into our country, and we are obviously trying to engage law enforcement in the People's Republic of China to assist us and to get information. Those are things that we do on a regular basis.

Again, I want to be clear that we don't have a matrix for success. I think I've been very clear that the relationship had been mute, so this is about re-engaging and starting that. I want to be very clear that this is not an endorsement of the particular country. However, there's work to be done from a law enforcement perspective. Regardless of the challenges, we need to work through those for the safety of our country and the safety of our citizens. That's incumbent upon us as part of our fiduciary responsibility.

Chak Au: Okay.

Again, in order to make our country safer, what kinds of guarantees do we seek from our partners regarding implementation or what kinds of measures have to be put into place to make it work? I don't want people to have a false expectation based on a useless MOU.

What kinds of guarantees are we seeking in order to make this kind of protection effective?

D/Commr Bryan Larkin: Generally, I don't think we go into any guarantee. When we enter an MOU with any law enforcement agency globally, there are no guarantees. There are no performance outcomes or matrixes in those MOUs. Their purpose is to create a framework and a regulatory opportunity for us as to how we can share information and how we can work collaboratively. At times, there's language around cost recovery in those MOUs. It's how we use the information. That's what it's designed to do. There's a broader perspective here. I don't think that any MOU that our organization has with any law enforcement agency has the outcome or guarantee that—

The Chair: I'm sorry, but—

Chak Au: Why not take it one step further than the MOU?

● (1745)

The Chair: I'm sorry, but I have to cut you off because we're well over time. Thank you.

MP Ramsey, go ahead for five minutes, please.

[*Translation*]

Jacques Ramsay: Mr. McCrorie, when we were interrupted, you were in the middle of answering my question.

What is the CBSA's plan for training the 1,000 officers you have to train? Does the agency have the funding to start the training in the next year? Does it have the schools and physical resources it needs?

I have a supplementary question. How will those 1,000 officers be allocated? How many will be assigned to port, land, rail and airport border crossings? How many will be assigned to defence?

[*English*]

Aaron McCrorie: Thank you for the question.

Yes, we're on track to hire our 1,000 officers by the end of fiscal year 2028-29. As of May 8, we had over 100 of the 1,000 new officers in place, and 200 will be in training at the college in Rigaud by July.

In terms of your question on infrastructure, management at our college in Rigaud has looked at both our attrition and the need to bring in new staff to meet that commitment for the 1,000. That is part of what they're doing. That is what their plan is, so we're well on track to do that.

In terms of allocation, about 800 of the officers will be uniformed officers allocated to points of entry—for example, land borders, marine ports and rail facilities. We're working through the exact disposition as staff come on. As I mentioned earlier, we'll be doing that on a threat or risk basis. It's where they're most needed. I'd describe the roughly 200 others as operational staff. They'll be brought on as well. We've started to assign them. For example, in my particular organization, I'll have some staff assigned to doing security screening. In the broader program that I'm responsible for, we'll have criminal investigators and people doing inland investigations.

Those staff are coming on board, and we're on track to meet our commitments.

[*Translation*]

Jacques Ramsay: Thank you.

Mr. Pyke, I want to talk about intercepting the contraband that comes into prisons. You hear a lot about that when you visit a facility. I gather it requires a lot of effort and resources, and it's expensive.

What is Correctional Service Canada's plan? Do you have a strategy for each institution or an overall strategy? I'd like you to speak to that.

[*English*]

Jay Pyke: Thank you very much.

Yes, we have an overall strategy. Every site has drone-detection systems right now. The issue is this: It's one thing to detect a drone and another thing to interdict it, in the sense of being able to stop the payload from coming in. We have now introduced new technology for drone mitigation. We intercept the signal. We just finished our first pilot site in Ontario. The next site is in Quebec. We're moving forward with the ability to prevent drones from entering our airspace, which will stop the payloads, the drops and the like.

There's another piece to this too. It's technology, so we have to constantly be updating. Typically, you might have had radio-frequency drones, as an example. Now we're seeing more GPS waypoint and cellular drones. We're always evolving the technology.

I am very happy to report that, after the spring economic update, we received $60.4 million, all of which will go towards drone mitigation and cellular mitigation for this very purpose. It's the number one thing we're seized with in terms of contraband entering our institutions across the country. We're also receiving just over $2 million, ongoing, to support those systems in place.

The goal is to be able, within three years, to detect drones, have drone mitigation and prevent drones from entering our airspace, and to mitigate cell signals at all of our establishments.

[*Translation*]

Jacques Ramsay: Do you plan to use physical elements as part of that strategy, such as moving windows further away or even making them harder to access?

[*English*]

Jay Pyke: Absolutely. That's part of the layered approach that we're using. There are different layers. It's one thing to mitigate the interdiction of contraband through technology. There's also old school: physical presence, dynamic security and physical measures. Sometimes we use netting. We reinforce windows. We reinforce areas so that they can't break through because, believe it or not, some of the drones will actually fly to a specific window. It's to be able to reinforce areas so that they can't get into those for certain.

In terms of general infrastructure upgrades, yes, we're in dire need of infrastructure upgrades. Within the Correctional Service, a lot of our infrastructure is older. It was not built or designed with the idea of drone technology, for example, coming in, so a lot of our upgrades consider those pieces.

● (1750)

[*Translation*]

The Chair: Thank you very much for those comments.

Given the time, I suggest we suspend the meeting, so the witnesses can take their leave and we can get ready for the third hour.

I want to thank all the witnesses for making the effort to be here today. Enjoy the rest of your day.

Honourable members, please be ready to start the next hour very soon.

The meeting is suspended.

● (1750)

(Pause)

● (1755)

The Chair: We are now resuming.

For this third hour, we will be turning our attention to Bill C-22, as you know.

We have a number of witnesses here, some of whom the committee is familiar with. I'll introduce them quickly. From the Canadian Security Intelligence Service, we have Ramzi Nashef, director general. From the Department of Justice, we have Kimberly Gibner, deputy assistant deputy minister; and Normand Wong, acting general counsel. From the Department of Public Safety and Emergency Preparedness, we have Richard Bilodeau, senior assistant deputy minister; Shannon Hiegel, director general; and Fenton Ho, director. Lastly, from the RCMP, we have Richard Burchill, chief superintendent.

We can move right into questions from members, starting with Mr. Caputo.

You may go ahead for six minutes.

[*English*]

Frank Caputo: Thank you very much, Mr. Chair.

Thank you to the officials here.

The government is in the process of drafting amendments. Have any of you seen those amendments?

Richard Bilodeau (Senior Assistant Deputy Minister, National Cyber Security Directorate, Department of Public Safety and Emergency Preparedness): Yes, it's part of the process. We haven't seen every amendment that's come in, because they go through the committee and we don't see those, but we do contribute to that.

Frank Caputo: Okay.

Are you able to talk about the government amendments that you've seen?

Richard Bilodeau: I'm not at liberty to do that.

I can refer you to the minister's comments yesterday in terms of the amendments he was contemplating and he announced.

I understand that there's a process for amendments to be moved here at committee, and we will be happy to come back and provide our factual support in your consideration of those.

Frank Caputo: I'll continue with you, Mr. Bilodeau.

You have been attuned to the fact that there's been a great deal of criticism of this bill. You'd agree that much of that has surrounded part 2. Is that correct?

Richard Bilodeau: It's definitely the part that we at Public Safety have been the most involved in. The discussions that I've had have been surrounding part 2.

Obviously, you've noted the coverage and the discussions. I think, statistically speaking, that would be accurate.

Frank Caputo: If we're being candid, part 2 deals with encryption and the lack of safeguards therein for encryption. Part 2 also leaves nearly everything to a ministerial order that can be secret, and part 2 fails to identify and define the precise categories of metadata. When I say precise categories, it's that metadata being kept for 12 months. Those are just three of the issues.

Would you be in a position, Mr. Bilodeau, to make suggestions or to comment on whether this bill could be split along the lines of part 1 and part 2?

● (1800)

Richard Bilodeau: That is not for me to opine on.

The bill that's before Parliament right now in this committee has a part 1 and a part 2.

You talked about what's in and what's out of the legislation. The legislation is intended, as we've talked about, to be a framework that leaves some of the implementation to regulations, not just ministerial orders. There are set things that will need to be put in regulations, like core providers, some of the capabilities and what kinds of metadata will have to be retained in that context for up to a year.

It is intended to be a piece of legislation that brings a regulatory framework to ensure that it keeps pace with what's happening out in the digital world to help and support law enforcement.

Frank Caputo: My reading is that a minister could designate a core provider through a ministerial order. Is that correct?

Richard Bilodeau: The legislation, in proposed section 5, provides for core providers to be designated through regulation through publication in the Canada Gazette. That's how core providers are defined as part of the legislation. There are criteria, as you know as well, that set that out. Then ministerial orders can also be used in a way to ensure that potentially targeted providers are able to put in place certain other requirements of the legislation.

Frank Caputo: Okay. I'm sorry; I was thinking about something else. I'll move on from that.

What I'd really like to know about is end-to-end encryption. We all know what that means. A number of companies use encrypted technology. Let's say it's Apple Health or something like that. We could agree that's very personal information that would be contained on your smart phone about your health. I don't think anybody's going to dispute that. It attracts a high expectation of privacy. Let's say that's encrypted. That's different from end-to-end encryption. A company like Signal offers a service that goes from one end to another and nobody can break it. That's end-to-end encryption.

What about when data is encrypted as part of the program? If Apple has the key to that encryption, would they not be required to track that data as part of this bill?

Richard Bilodeau: You're correct that there are different types of encryption that can be done end to end if there's a communication. It can be user-encrypted. It's not just about communication. A user could have their own encryption where the provider does not have the key to that information. There are encryption models where the supplier or provider may have the key to that encrypted data.

I can't speak to the Apple example. I'm not a technical expert in terms of what each company does and how they do encryption.

Frank Caputo: Hypothetically is what I'm getting at.

Richard Bilodeau: I understand that.

For the legislation, in your example, it does not automatically provide that the provider—Apple, in this instance—would have to keep data. They would have to be designated either as a core provider or through a ministerial order. That process would need to happen before any obligations were imposed on them.

Frank Caputo: My point though, sir, is this: It could happen.

What I'm getting at is that information that is meant to be encrypted and is itself encrypted could be compromised beyond end-to-end encryption. We're not just talking about end-to-end encryption because we were told that would introduce a systemic vulnerability if somebody had to disrupt that. I'm talking about data that is encrypted, but there is nonetheless a road map to it in the provider.

What I'm saying and what you're telling me that's of concern is that encryption that is not end-to-end that is provided by the service provider could then be subject to this bill. Do you get where I'm going with this?

Richard Bilodeau: I understand, yes.

Frank Caputo: Is that not accurate? Basically, what I'm asking is this: Isn't encrypted data still subject to this bill?

● (1805)

The Chair: Give a quick reply, please.

Richard Bilodeau: If there were a judicially authorized warrant to access information, then it would depend on where the information lies, where the encryption is and also whether the regulations or orders apply.

It is case-by-case. It's hard for me to speculate on a hypothetical, because it would depend on the requirements set out in the regulations that we would be developing in consultation, and in the context of ministerial orders, with the provider—because it's a part of the legislation that we need to consult with them.

I would also say that in the context of the ministerial order, the provider could refuse to do it if it introduced a systemic vulnerability.

Frank Caputo: In this case—

The Chair: Thank you for that. There will be other turns.

Next is MP Sodhi for six minutes, please.

Amandeep Sodhi: Thank you, Mr. Chair.

Thank you to all of our witnesses for being here today. My first set of questions will be directed to Mr. Nashef from CSIS.

To begin, to what extent do you believe Bill C-22 will bring CSIS's capabilities closer to matching those of our Five Eyes partners?

Ramzi Nashef (Director General, Policy, Planning and Accountability, Canadian Security Intelligence Service): Thanks for the question.

In fact, that's the exact objective of the bill from CSIS's perspective. As has been mentioned here many times today, we're the only Five Eyes country and one of the only like-minded countries—if we want to use that term—if we compare ourselves to the Europeans, that is absent a lawful access regime. For us, this would be a significant bound to put us in a position of equal footing with partners in terms of what we are able to get under judicial authorization.

Right now, to make a quick point of it, we rely on ad hoc arrangements with a range of different electronic service providers that give us an unpredictable and widely varying set of outcomes depending on which region of the country and which provider it is we're working with on any given warrant, let's say. For us, this is a significant step that will put us on much closer to even footing with key partners.

Amandeep Sodhi: Thank you for your answer.

We've had some people say that this bill will create some sort of a cybersecurity risk. What would be the cost to national security if we don't pass Bill C-22, particularly as encrypted communications become the default for threat actors?

Ramzi Nashef: That's another good question.

There were some questions earlier today around the risks of the bill. Something that has not necessarily been discussed today is the risk of not having a lawful access regime in this country. It's been a 30-year journey to get to the point of maturity of the current bill in front of you, and that has been with significant ups and downs.

The cost is increasing, to be frank with you. You can hear it from me, from CSIS and from counterparts on this panel. Don't necessarily take our word. There are other significant cross-partisan analyses, including the NSICOP report on going dark, that really get to the heart of the costs.

I would say that the slippage we are seeing, even when we have a federal court warrant for the information we are authorized to get but still cannot get, is increasing. That gap, for us, is an immediate and tangible one in terms of the safety of Canada and Canadians from what, for CSIS, for example, are the highest harm threats. We're talking about espionage, foreign interference and terrorism, primarily. That cost is here, and it's increasing. This bill is a significant proposal that would really modernize that set of tools for us.

Amandeep Sodhi: As you're aware, Peel Regional Police recently laid more than 100 criminal charges in what investigators described as one of the largest extortion cases in the region's history. It involved violent extortions targeting members of the South Asian community and their businesses.

How would lawful access tools improve CSIS's ability to investigate those networks more efficiently?

Ramzi Nashef: I'll give a general answer and then pass it to my colleague Chief Superintendent Burchill.

For us, it's about being able to advance investigations and get better investigative outcomes in a quicker time frame. As I mentioned previously, we are only talking about the highest-harm threats. As such, it is of particular importance that we're able to improve the investigative outcomes because, as has been raised by the minister and many other speakers today, that erosion has been significant. It's been over decades, and we are really at an inflection point where a significant improvement and a modernization of those tools is required.

To speak specifically to the types of crime you mentioned, I'll pass it to Rick. Thanks.

● (1810)

Chief Superintendent Richard Burchill (Director General, Technical Investigation Services, Royal Canadian Mounted Police): Thank you very much for the question.

From a law enforcement perspective, the Peel case represents the capability they had to get the evidence and bring charges, but with the number of extortion cases across the country, we have a national task force assisting police of jurisdiction, as well as RCMP where we're the police of jurisdiction, to try to have more better outcomes. The way that extortion cases unfold is particularly complex and difficult from a lawful access perspective, so having the tools that this legislation would provide would certainly enhance those investigations and provide better outcomes for law enforcement.

Amandeep Sodhi: I want to turn to the officials from the Department of Justice.

Apple recently testified that “anyone can walk through” a back door, but Bill C-22 requires that providers be capable of executing a lawfully issued warrant.

Can you clarify for the committee the legal distinction between a back door and a court-supervised lawful access mechanism?

Normand Wong (Acting General Counsel, Policy Sector, Department of Justice): Thank you for the question.

A back door, the way that I understand it, is the systemic vulnerability that we've been talking about in relation to part 2.

Lawful authorizations, as our colleagues from CSIS and the RCMP have said, are obtained from the court. This is when police or national security is required to get a warrant. There are certain requirements to obtain that warrant in terms of evidence. The issue is that we have many of the tools already in the CSIS Act and the Criminal Code that allow our authorities to gain access. The problem is that when they go to the service provider, the service provider cannot allow them access.

Amandeep Sodhi: Thank you.

Thank you, Mr. Chair.

The Chair: Thank you for that, MP Sodhi.

[*Translation*]

It is now over to Mrs. DeBellefeuille for six minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Thank you to the witnesses for being here.

Mr. Bilodeau, I'm going to tell you the feeling I have. In light of what the witnesses have told us, the sense I've gotten since the beginning is that they don't understand the bill. Their comments put all kinds of doubts in our minds. For your part, you're saying that isn't the purpose of the bill. When you say it enough times, it's almost like you're telling us we should trust you because that isn't really the bill's intent.

As I see it, things would be clearer if you spelled out in the bill everything people don't understand. That would make us feel better, especially about the whole issue of back doors. Basically, apart from the police services, hardly any of the organizations and companies we met with agree with some of the provisions in Bill C-22. To my mind, one of your responsibilities is making sure that the committee has a clear understanding of the bill, so you need to stop saying that isn't the purpose of the bill and, instead, lay out exactly what the intent is right in the bill.

After hearing everyone's concerns, I'm very hopeful—I know the government would like to achieve somewhat of a consensus on Bill C-22—that you'll have a chance to clarify things.

I wanted to say that at the start, because, as a parliamentarian, I don't have the expertise of a computer scientist. There are all kinds of things I don't know, so I'm relying on the experts, and all the experts are telling us that if Bill C-22 is passed as is, privacy will be no more. I can name plenty of people who said so.

Do you think it's important to include clear definitions or perhaps even who the bill does not apply to? That's another suggestion we got, from Desjardins and Interac, who wondered whether they would eventually find out if the bill applied to them, since the definition will be established by regulation.

Are you working on anything or having any discussions that will provide us with the details we need regarding the government's intention? Those details are necessary to inform our consideration of Bill C-22.

● (1815)

Richard Bilodeau: Thank you for your question.

I believe the minister said this yesterday when he spoke. We, too, have said a number of times that, if it's possible to provide clarity in the bill, as parliamentarians, you will have the opportunity to make amendments.

The government stated yesterday that it would do that and provide some clarity. With respect to end-to-end encryption, for instance, not being able to introduce systemic vulnerabilities is precisely the issue, in our view. The legislation does not allow end-to-end encryption. It is clearly excluded. The government said it wanted to clarify that.

Quickly, something worth considering is that the bill really creates a framework to specify who the legislation applies to. For example, in the case of core providers, there is a process to follow. It's a transparent process. Consultations will take place. The regulations will have to respect certain criteria throughout. The same goes for ministerial orders; the matter will have to be discussed with electronic service providers first.

Putting everything in the bill wouldn't necessarily allow the act or regulations to keep pace with technology. That's why the bill is drafted the way it is. Considering how technology is adopted—

Claude DeBellefeuille: I understand, Mr. Bilodeau. Essentially, in the regulatory part, you're suggesting we be more agile so we can adapt quickly to changes. The problem is that the police forces and the RCMP often tell us they've been waiting for this for 30 years.

In my view, the United States and the United Kingdom aren't good examples when it comes to privacy protection. When people tell me we should copy them, I become wary, because here in Quebec and Canada, we have a strong culture of privacy protection. We understand the needs of police forces, but before approving of this legislation, we want to be sure that everything is in place to meet police officers' needs while providing safeguards.

I understand the regulatory part, but could we proceed in stages? What I mean is this: We adopt the bill with certain clarifications, and then we'll revisit it in two years to refine and improve it based on how it has worked in practice.

Adopting Bill C-22 represents a major cultural shift. Just because we're not like the others doesn't mean we're not good. Maybe we're the best at protecting privacy, and we don't want to imitate those we don't admire. That's what I'm after.

Do you think it would be possible to proceed in stages?

Richard Bilodeau: To answer your question, I'd say that it will have to comply with the Canadian Charter of Rights and Freedoms, whether it be the bill or the regulations.

We created a bill in response to information obtained by our allies, whether from the Five Eyes or from European countries, but we have drafted it in a Canadian context, in accordance with Canadian laws. We have a charter here in Canada. Laws must therefore comply with the charter. Our colleagues at the Department of Justice have submitted the required statement of compliance with the charter.

Whether at the level of the act or the regulations, it has to comply with the charter. There are also privacy requirements that must be considered in developing regulations and ministerial orders. We think we've struck the necessary balance by implementing ways to respond to the needs of police forces and the Canadian Security Intelligence Service's requests. In the end, these measures protect victims of crimes and national security threats, but they do so in a way that respects privacy and the Canadian Charter of Rights and Freedoms.

The Chair: Thank you for your thoughts.

Ms. Kirkland, you have the floor for five minutes.

[*English*]

Rhonda Kirkland: Thank you, Chair.

My first questions will be directed to Mr. Nashef.

Thank you for being here today. I'm appreciative that you're here because I've found that any time I've asked questions of you in the past, whether it's in this committee or otherwise, you speak in a language that Canadians understand. Sometimes it is very hard for people to truly understand what's going on with technical pieces.

I have some important questions.

Would CSIS consider a government-mandated access point within an encrypted system to be a vulnerability from a cybersecurity standpoint, even if it's authorized and controlled?

Ramzi Nashef: You might have jinxed me with the front end of your statement—

Rhonda Kirkland: No.

Voices: Oh, oh!

● (1820)

Ramzi Nashef: —just in the sense that there are a lot of layers to the question you just asked me.

In fact, not to challenge the premise, but it would be my view that we're not asking for a government-mandated access point. It would be, again, intercept-capable. That's the language we would use.

Rhonda Kirkland: Thank you. That helps me. That answers my question.

Would you agree, though, that any mechanism created for lawful access is inherently dual-use, so it could potentially be discovered or exploited outside authorized use?

Ramzi Nashef: There is no technical system by any means that is 100% foolproof by any stretch. The only small footnote I would give you there is that.... Well, I might leave it there, and I'll let you keep going.

Rhonda Kirkland: Okay. I may ask you about that footnote later.

Has CSIS assessed whether large-scale metadata retention creates a higher-value target for foreign intelligence services or cybercriminal groups?

Ramzi Nashef: It wouldn't necessarily be a CSIS assessment there. It would be a national security partner that would have the more centralized expertise on the cyber side. My short answer would be, yes, that's a thing that has been considered and thought through.

I would maybe offer my footnote now, because I teased it. I think the point I started with is the point I will start with again here, and then I'll finish with a second one. It is that, no, there is no technical system that is 100% foolproof by any stretch. We have heard what has been said here and take the point. I would say also, though, that you have a group of people who work in a national security community, whose fundamental ethos is to protect Canadians, Canadian systems and the critical infrastructure of this country.

Rhonda Kirkland: Perfect. That's understood. I'm coming from a place of helping Canadians understand this and helping them feel like they can trust it.

On a human level, one to one, when you're talking to anyone, they would feel like large-scale retention of metadata would be a higher-value target. Put yourself in the place of a bad guy. You're a bad guy—it's a higher-value target.

Ramzi Nashef: Yes.

Rhonda Kirkland: Mr. Bilodeau, the public safety minister has mentioned that the metadata provision will be brought in line with U.S. law, but the American lawful access statute, CALEA, imposes no data retention requirement at all. It's an interception regime. It requires providers to be able to hand over communication under a warrant. It does not require them to stockpile metadata in advance on everyone, just in case. There's nothing in U.S. law resembling the up-to-a-year, suspicionless retention this bill contemplates.

Can you be specific on which U.S. statute he would be referring to that would get us up to date and in line with U.S. law?

Richard Bilodeau: I think that statement may have been corrected following the minister's remarks. What I understood it to mean, or what was said during that conversation, was really about bringing encryption in line with CALEA. It has specific language around end-to-end encryption and not being able to force providers to decrypt end-to-end encryption. That was the intent of that statement.

Rhonda Kirkland: That brings to mind, then, Mr. Caputo's question, because I'm finding myself, as many Canadians are, not as technical and not understanding. End-to-end encryption I understand. However, there are encrypted items on my cellphone right now that are not really end-to-end encryption so....

Richard Bilodeau: The distinction that the legislation makes is that if an electronic service provider does not have the capability to decrypt your data, because your device has encrypted the data on your phone and they don't have the key, so to speak, then the legislation can't force it, because the supplier or the provider does not have the capability to do it. There's a distinction based on where the data is encrypted.

Rhonda Kirkland: Would it—

The Chair: Thank you, Ms. Kirkland. I'm so sorry.

We'll go to MP Housefather for five minutes, please.

Anthony Housefather: Thank you very much, Mr. Chair.

I think this is a good opportunity for us because we have to prepare amendments to the bill. One amendment that I think is very important is the one that Ms. Kirkland was just talking about. It's with respect to encryption and bringing this into line with the U.S. statute to say that no company that doesn't have a key to the encryption has to create one or could be ordered to create one, under an order. I think that's very important, but another element that is important to look at in this bill is the systemic vulnerability issue, the definition of systemic vulnerability and its interplay with the orders.

I think it will be relatively simple to craft amendments to say, for example, that you can't be forced in an order to create a systemic vulnerability. I think we can create amendments to do this that would be very agreeable.

I have an issue with the definition of “systemic vulnerability”. This is what it says right now:

> systemic vulnerability means a vulnerability in the electronic protections of an electronic service that creates a substantial risk that secure information could be accessed by a person who does not have any right or authority to do so.

A substantial risk is very high. It means it's not just any risk. It's not a plausible risk. It's not just a risk. It's not a material risk. It's not a real risk. It's not a credible risk. That's a lower threshold. It basically means that if somebody says, “I think there's a plausible risk that by doing this we will create a systemic vulnerability”, they could still be forced to do it.

I'm not satisfied with “substantial” risk. I understand that there may be a reason to not just remove the word “substantial” and put in “a” risk, because that would be any risk, irrespective of how immaterial it is. What word should I propose, or do you recommend that I propose, as an amendment?

For example, if I were to use “plausible” risk, what, then, do you believe would be the legal interpretation? How would that be viewed? What would be the effect?

● (1825)

Richard Bilodeau: That's a good question. I might ask my colleagues from the Department of Justice to weigh in. I'll give them an opportunity to think about it.

At the end of the day, substantial risk was used to strike that balance between providing a framework for lawful access and making sure we're not creating those systemic vulnerabilities. The last thing we want this legislation to be used for is to weaken this. As one of the previous witnesses said, we don't want to harm Canadian security writ large, whether it's through this or cybersecurity.

That's why I would add to Mr. Nashef's answer earlier that a lot of data is being retained now. Companies are used to doing this. They take a lot of precautions. Some of the firms have very good cybersecurity hygiene and take really important steps to protect that. We would expect that to continue under this lawful access regime, because some of the data might still be kept.

Anthony Housefather: I agree, but then you're speaking to why we shouldn't be using the threshold of substantial risk. Substantial risk means you could be asking to do something. They could say, “I think there's a real risk here, a plausible risk”, and they're still forced to do it.

Coming back to my question, if I said “plausible” risk, what is the position of the Department of Justice on what that would mean? Would that make any change that would undermine the purpose of this legislation?

Normand Wong: Thank you for the question.

I don't know if I'll be of much assistance on this, Mr. Housefather. You have highlighted the fact that a variety of words can be used. I think you rightly point out that it will change the scale. At the end of the day, it's a policy decision, how this is decided, and it's the Minister of Public Safety's responsibility in that part of the act.

[*Translation*]

Anthony Housefather: Since I only have one minute left, I'll just follow up on something from earlier.

I understand what the witnesses are saying; it's all very clear. I think we have to be responsible, but without requiring a company to do something that could plausibly create a risk, as the company mentioned.

So if you can't suggest another word, I'm going to continue to use the word “*plausible*”.

Mrs. DeBellefeuille, is “*plausible*” the right word in French?

Claude DeBellefeuille: Yes.

Anthony Housefather: So, if I use this word, do you think it is going to create a legal issue by preventing the government from obtaining the information that police forces or others really need?

Richard Bilodeau: Mr. Chair, from a non-legal standpoint, that is, simply from a linguistic point of view, the words “*plausible*” and “*un risque important*” don't mean the same thing to me. The word “*plausible*” evokes the likelihood that something will occur, so the level of risk is much lower. It's not in the same category as a substantial risk. They might not be synonyms. I don't want to pull out my French dictionary, but these words don't necessarily belong in the same category.

● (1830)

Anthony Housefather: It's not about whether or not they're in the same category, but rather about what they mean for the company. If we say that a risk is plausible, then it isn't substantial.

Richard Bilodeau: A plausible risk could suggest the likelihood of it occurring, regardless of the risk level. I think it's up to you as parliamentarians to decide how you'd like to move forward. However, there is a difference between the two.

The Chair: Thank you very much. That was all very clear and quite useful, I'm sure.

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Mr. Chair, I'm pretty impressed. As you can see, all parliamentarians across all parties want to understand the issue in order to adopt the best possible bill. The questions are coming from all parties, even the governing party. We want to adopt an important bill, which we know will bring about a cultural shift in Quebec and Canada. We want to make sure we improve it.

I find Mr. Housefather's questions relevant, because we're looking for the right words. We want to make sure we use the right word to reflect the government's intent or that of Public Safety Canada.

Mr. Bilodeau, I'd like to talk about metadata, because all of the witnesses have brought up the risks associated with such long retention periods. We've had discussions about this.

While studying the bill, I had an idea. In the regulatory section, we could say that the data will be kept for up to a year. That doesn't mean that all of the data for every Quebecker and every Canadian would be kept for a year. This may be something you wish to address in the regulatory section. However, not mentioning it and not putting it in writing creates confusion or insecurity and, I'd even say, a lack of trust.

I think that if you don't intend to keep 100% of Canadians' data, this should be stated explicitly in the bill in order to reassure people. As it stands, this is what it says. It doesn't say “up to”, “depending on the category” or “depending on the type of data”. Do you think there's room in the bill for us to clarify this?

Don't ask me to draft an amendment, because I wouldn't be able to do so. I'm asking whether there is somewhere this clarification could be added.

Richard Bilodeau: It is certainly true that clarifications can always be made to a bill. I will leave it to parliamentarians to propose such amendments.

As we have said on several occasions in different forums—and I believe we have discussed this with you as well—we are really looking to extract and define the metadata that will be useful for investigations, as well as a retention period for that data. That could be up to a year or less, depending on the type of data. You are absolutely right.

If you'd like, we can discuss the need for certain types of metadata. My colleague from the RCMP can explain why retaining metadata for up to a year may be relevant in the context of an investigation. Often, investigations do not develop in such a way that, from day one, a decision is made to obtain all the metadata relating to a person suspected of having committed a crime. This retention period is therefore necessary.

We are really seeking to address the current gap, where some providers do not retain metadata for longer than a week, while other electronic or telecommunications service providers retain it for much longer than a week. There is already data in the system that is retained for longer periods.

The Chair: Thank you very much.

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

[*English*]

Frank Caputo: Thank you, Mr. Chair.

I want to pick up on what Mr. Housefather was talking about. I wasn't planning on going into this, but he makes a very good point.

If I understand his point correctly, and maybe I don't, what I understand is a general concern. Who says “substantial likelihood” or whatever it is? What about a “possibility” or “plausibility”? If I could make one suggestion or one thought, it's that business hates uncertainty. The uncertainty in this bill is what's driving business to come out so clearly.... Even if it's a possibility, then what a business.... If I'm a business owner or if I'm advising shareholders or whatever and I have uncertainty, and it's “possibility” and they say, “Well, the recourse is that you have judicial review”, well, somebody might disagree with you.

What I want to underscore to the officials is that uncertainty is so pronounced here. When you are advising the government, please recognize that. Even with metadata, we don't know what classes of metadata will be preserved for up to a year. A point that's been made here is that we don't need to preserve anything for a full year. Which is it? I get that you want to put it in regulation and I get that it changes, but the act is silent on those things.

I'll open it up for comments, and then I have a question on what I had to say. Does anybody have any comments on that?

● (1835)

Richard Bilodeau: You mentioned regulation. For the first class of core providers, there's always going to be a first in the regulation. It will be clearly set out in the regulations what metadata needs to be retained and for how long.

Frank Caputo: I'm aware of that, but that's precisely my point. We around this table don't know what that's going to look like. I get that's how regulation works, but the uncertainty.... Again, we come back to that word “uncertainty”, because it's for up to a year. We don't know what type of metadata is going to take priority. We don't know whether location services are going to be there for up to a year.

A year is a long time. I understand that the argument has been made that we need this, but no one has asked, “Why a year?” That's another point. We have asked about industry standards. Australia has two years. Sweden has 10 months. There are also nuances there, but there's that uncertainty again.

Another reason for uncertainty is in proposed section 14, and that is the duty to assist. If I was a business owner, I think that I could rightfully fear this. Does proposed section 14 not conceivably require an electronic service provider to create hardware or software to bring it up to government standards, so to speak, so that the data can be retained? I hope that question is clear.

Richard Bilodeau: I'll ask my colleague Ms. Hiegel to respond.

Shannon Hiegel (Director General, National Security Policy Directorate, Department of Public Safety and Emergency Preparedness): Absolutely. The expectation is that we are setting a standard across the current practices that is ad hoc. It is based on individual agreements.

Take the telecommunications class, as we call it. They are not all the same. When law enforcement goes to one provider over another one within the telecommunications world, they don't know if they're going to get the same information. If you're running an investigation and you're six months into something, it's probably taken you six months just to figure out which telecommunications provider it is. You're going to get a different set of information from different telcos. That is fundamental within setting a regulation. It's more than an expectation. You know what you get—

Frank Caputo: You want uniformity there. When we need information, we want to know it's there. I get that, but when I read this, if you're a small ESP, it might cost a million bucks to get up to that level. How do we, as parliamentarians around this table, say, “I get why you want uniformity”, but when we are sitting around this table, how do we address that for a small ESP?

A million dollars might be the smallest amount they have to pay, but that could cripple a company of that size. How do we respond to that?

Shannon Hiegel: One of the key elements.... Again, I am going to use the word “regulation”. In deciding who a core provider is, one of those factors is going to be how big your client base is. Are you national? Are you regional? How regional are you? How small are you? What is the service that you provide? There needs to be a very detailed conversation with these companies, so we can make a well-oiled regulation.

Frank Caputo: Therein is the issue. It is the uncertainty right there. Yes, we're going to factor these things in, but even factoring them in, you and I can't decide what that would look like. That uncertainty, I think, is what is driving a number of the questions here.

● (1840)

The Chair: Your point is really well made in a short amount of time. Thank you.

[*Translation*]

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

[*English*]

Jacques Ramsay: I will leave the floor to Mr. Housefather for the next question.

[*Translation*]

Anthony Housefather: Thank you very much, Mr. Ramsay.

[*English*]

I'm going to come to the exact same point that Frank and Claude elaborated on.

If I was to say that, instead of “substantial” risk, it's a “credible” risk based on objective professional standards—so we now have assessed what the level of risk is and what it's based on—can the people from justice please tell me if that would be inconsistent with wording that we have in other legislation?

Kimberly Gibner (Deputy Assistant Deputy Minister, Policy Sector, Department of Justice): Thank you for the question.

I think you've posited something really important to think about. We haven't thought about it and we're certainly open to what you—

Anthony Housefather: Would you be willing to exchange with the committee on that?

I think I'm going to prepare something on that level and I'd be very interested to hear from you.

[*Translation*]

Thank you very much.

I'll hand the floor back to Mr. Ramsay.

Jacques Ramsay: Is anyone among the witnesses familiar with the brief submitted by the Privacy Commissioner and the recommendations it contains?

The committee hasn't had much time to review these recommendations. I would like to hear your views on them, particularly the fifth recommendation, which deals with the powers of the Governor in Council and the minister, and suggests that the obligations imposed be necessary and proportionate.

Richard Bilodeau: Thank you for that question.

We've taken note of the Privacy Commissioner's brief. A good portion of the criteria and language proposed by Mr. Dufresne would form part of the regulatory analysis, since privacy protection must be taken into account as a factor in the drafting of regulations and ministerial orders.

So that would form part of the regulatory analysis.

Jacques Ramsay: So we have to take your word that it will be considered at a later stage.

Richard Bilodeau: It's a criterion that is currently set out in the legislation.

Jacques Ramsay: Let's talk about the sixth recommendation.

We are well aware that a provider has the ability to invoke a systemic vulnerability. The sixth recommendation calls for the government or the minister to be unable to require anything that would introduce a systemic vulnerability. That is a request which, I believe, is at a higher level.

Richard Bilodeau: The intent of the sixth recommendation is to place the burden on the government to determine whether a systemic vulnerability exists.

In the analysis we conducted while drafting the bill, we concluded that this analysis would be better carried out by electronic service providers, because they know their systems better than anyone—certainly better than the government—since they are the ones who developed and operate them. It's therefore up to them to tell us whether what we're asking them to do could create a systemic vulnerability. We would then hold discussions and decide, based on this information, whether the ministerial order should be issued in the form considered initially.

We will use the information provided by the providers to make informed decisions. We truly intend to consult with electronic service providers, and this is not merely an intention; it is a requirement under the legislation.

Jacques Ramsay: Under clause 12, it states that a provider subject to an order is required to comply with it. In the event of judicial review, is there a way to stay this order, or must the provider proceed regardless?

If the provider must proceed regardless, the commissioner's recommendation would make sense.

Richard Bilodeau: My understanding of clause 12 is that it does not override the obligation not to introduce a systemic vulnerability. Therefore, clause 12 cannot require providers to do something if there is a systemic vulnerability.

Jacques Ramsay: Yes, but if it's being challenged, that means we're going to judicial review. At that point, does the provider have to proceed while waiting to ultimately be found to be in the right, or can it avail itself of that recourse and say that it will wait for the judicial decision?

● (1845)

Richard Bilodeau: My understanding of judicial review is that the provider could request a stay of the proceedings while the review is under way. There is the criterion of irreparable harm and all of that, which may come into play.

However, I will turn to Ms. Gibner, who can provide you with more context.

The Chair: Please answer quickly, Ms. Gibner, because we need to move on to another intervention.

[*English*]

Kimberly Gibner: Yes, I'll simply say that my colleague has done a great job of setting it out, and that's correct.

[*Translation*]

The Chair: Very well.

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

[*English*]

Chak Au: Thank you very much.

I don't know who can answer this question.

There has been much discussion about how long and how the suppliers should maintain the information, but here's another aspect. Once the information gets out of the hands of the supplier and into the hands of the police, how are they going to deal with that information? For example, where and how and for how long are the police going to keep the information? Also, when will they destroy the information?

There could be different scenarios. Number one, if the RCMP suspects that a person may have committed a crime and gets the information from the supplier and then at a later date discovers that this person is not really engaged in the criminal activities, when will they destroy that information about the person?

Secondly, will the person be informed that their information was given to the RCMP, and will there be some verification that the information has been destroyed?

Richard Bilodeau: I'm going to my colleague from the RCMP, who can answer all of those questions.

C/Supt Richard Burchill: Yes. Thank you very much for the question.

What I could say is that when we get to a point where there is a crime that we're investigating and we get to the point where we're dealing with data, then we're into a judicial authorization that a judge has authorized. With that comes a return to justice. If we're authorized to seize the data, we go to a supplier, to a service provider, and they're able to give us what we have through the court order, we have to do a return to justice.

Generally, every 30 days we have to go back to court to say what we've done: first of all, what we went in to get specifically; then, what we took specifically, what we're currently doing with it and where it's stored for continuity of evidence; and then why we need to keep it for another 30 days. There are returns to justice and a return to court to tell them what we're doing and for how long we're doing it.

If at some point the judge decides or the investigators decide that we don't need to keep this data anymore, it's destroyed. I suspect that the investigators would advise a suspect that they're no longer being investigated and they've destroyed any evidence related to them, but there is a court process with the return to justice as part of a warrant or a production order, where we have to go back and report to court what we're doing with what we've seized.

Chak Au: In that case, you're saying that the person who was investigated would be informed.

C/Supt Richard Burchill: I guess it depends on the circumstances. If informing the person sacrifices the integrity of the investigation, probably not. If at some point there are charges laid and that person has been eliminated as a suspect or part of the file, then they would probably be notified.

Rest assured, I guess, that there is a process with the judicial authorization such that we need to go back to the justice every so many days. It's the judge who decides how often. If it's very sensitive or if it's information that they feel they want to keep more control over, they may require us to come back every two weeks. It's hard to say, but it's up to the judge.

Chak Au: This is not exactly the answer I wanted, but anyway, I will move on.

In scenario two of the person who was being charged but eventually was found not guilty, again, what would happen to the information that had been collected through this process about him or her?

C/Supt Richard Burchill: For the general disposition of exhibits at the end of a trial, whether conviction or no conviction, it would be to have a disposition. If there is a conviction, they would probably be retained, but if there is a stay or if the person is not convicted of a crime, there would have to be a disposition of those exhibits, with the court saying, “This is what we seized during the investigation and we're now going to be disposing of it” and giving proof of that disposal.

● (1850)

Chak Au: Good. Thank you.

I have another related question. We are being told that this new arrangement of lawful access is needed because of investigations and other kinds of necessity. I get that, but on the other hand, how can we prevent these kinds of measures from being seen as necessary?

At the end, they become measures of convenience because we're talking about two concepts: reasonable suspicion or reasonable grounds to believe. There's a difference there, and I would say the threshold for the first one, grounds to suspect, is lower, much lower than the grounds to believe.

Where would one begin and end? I would suspect that there would be grey areas in between. In that kind of situation, how can we be sure that this will not become a measure of convenience for the police to abuse, if I can use that word, in order to obtain personal information?

The Chair: Give a very short answer, please.

C/Supt Richard Burchill: I can assure you that reasonable grounds to suspect is at the very beginning stages of an investigation. The jeopardy associated with having somebody's specific metadata, that requires reasonable grounds to believe and a general production order.

I'd ask my colleagues from justice to correct me if I'm wrong, but once you get to the point where you're seizing data, you're into reasonable grounds to believe and there's a bona fide investigation, a victim and a crime attached to that. When you're—

The Chair: I'm sorry to interrupt. I'm being very rude, but that's unfortunately what we need to do.

We'll go to MP Al Soud for five minutes.

Fares Al Soud (Mississauga Centre, Lib.): Thank you, Chair.

Thank you all for being with us today. I am not a usual member on this committee, but it is a privilege to be with all of you given the importance of the topic at hand today.

I believe it was Mr. Nashef who mentioned earlier that we are the only Five Eyes nation, the only like-minded country, absent of lawful access.

I find with legislation like this there are always concerns pertaining to privacy, and that is of course always an important question. One of those concerns I find is this idea, this floating notion, that Bill C-22 would create some sort of mass surveillance or that it would allow law enforcement to access Canadians' information without legal authorization.

I'd like to hear you speak to that, Mr. Nashef, if it's possible, and I'm happy to open it to the rest of the panel if expertise allows.

Ramzi Nashef: Thanks for the question. I'm glad you raised it because I think it's one of the things that have been in most of the coverage and the testimony that probably most needs myth busting, to be frank, by this group here and others.

I'll speak from CSIS's perspective, but it also, I think, carries for law enforcement on this front.

There has been a lot of discussion about the retention-of-data considerations in the bill. To actually access that data, it goes without saying—it hasn't come up that much today but to reiterate—there is no direct access for either law enforcement or CSIS to any systems of telecommunication service providers, in fact, in the intent of the bill or the letter of the bill. We have that established.

For CSIS or for law enforcement to actually get access to that data.... This idea of mass surveillance gives you the sense that we are floating through and swimming in the waters of the data, looking at it, using it for things investigative or otherwise. None of that is the case here. What we're talking about is that there's a retention of a limited amount of data for very specific investigative reasons, which we can access only with, in our case, a federal court warrant, so it's a significantly high threshold in a high-harm investigation, as I mentioned earlier, related basically to espionage, foreign interference or terrorism.

That would be how I would frame it to you. It's a much narrower access to the data that is being collected for a very particular reason at a very high threshold with significant oversight.

Fares Al Soud: With this notion of the data storage being, of course, a sensitive topic but a very important one, how do you find this legislation addresses the challenge of data being stored outside of Canada, and what improvements does it bring compared to the current system we have?

Ramzi Nashef: I'm not sure I'm the best one to answer all parts of that question, but let me take a first cut and then somebody can come in with a bit of fire support.

I think taking a half-step back might be helpful to talk about the data storage. There have been a significant number of questions from MP Kirkland and some others—really necessary questions—asking whether that increases the risk of the government mandating specific companies to retain extra data than they would have from a proprietary perspective for a set of reasons.

The first thing I would say is that many of these companies, but not all, retain a huge amount of data for all kinds of different reasons, data that goes far beyond what we're asking for in this bill. In many cases, that's for billing reasons. In other cases, it's for marketing reasons. It's for a whole range of different motivations, let's say. On this idea of the fundamental culture of how data is retained in this country, I think we're already there. The number of times we or folks we know hit “accept all” in any given day is really high and should be scary. This isn't the Rubicon that we're crossing with this bill. This is the data-driven world we have been living in for a while already.

In terms of the vulnerabilities around requiring additional retention of data, the half-step back I'd like to take might be to look at the financial sector as a parallel. It's not a perfect comparator, but it's one that's, let's say, a little less charged than what we're talking about here.

In the financial services world, more records and better records are seen as an inherently positive addition of robustness. Again, it is incredibly important—and we have been discussing that today, and it is at the heart of what we are trying to do—to ensure that we are not introducing unnecessary vulnerabilities. I have said a number of times that no technological system is 100% foolproof and unable to potentially be leveraged in certain circumstances.

I think what we're talking about here, though, is proportional. It's reasonable. It's limited, and it's for very clear applications, which are, again, in our case, highest-harm national security investigations. In the case of law enforcement, they are highest-harm criminal and transnational organized crime applications.

The parallel of the financial sector, where the same thing for different reasons is seen as a net positive—whereas in this case, it is seen or at least has been bandied about a little, as an unnecessary vulnerability—gives us a bit of perspective that could be helpful here.

● (1855)

[*Translation*]

The Chair: Thank you, Mr. Al Soud. You're making a very good impression for your first appearance. There is a good chance we'll invite you back.

That brings us to the end of this third hour. Before we adjourn, I would like to inform you of a prerogative I am going to exercise. Like everyone else, I noted last time that we didn't have time to reach a formal consensus on the coming days. However, I heard very clearly that you would like a little more time to discuss this bill.

I will therefore propose that we hear from witnesses next Tuesday on Bill C-22 for two hours, that the deadline for submitting amendments be extended to 5:30 p.m. next Monday, and that on Thursday, June 4, between 3:30 p.m. and 6:30 p.m., we devote the first three hours of our session to a clause-by-clause consideration of the bill.

On that note, I wish you all a good evening. Thank you.