HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

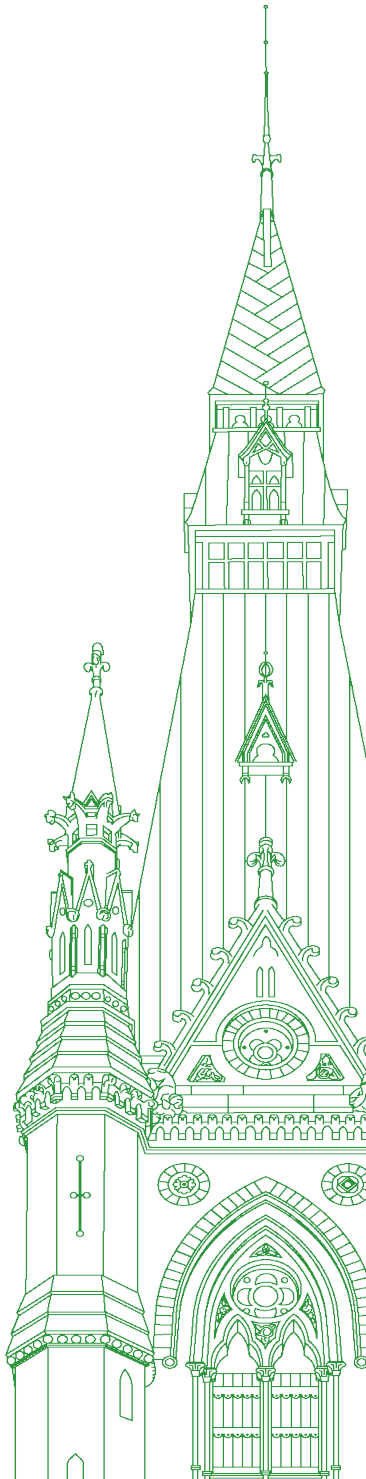
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 051

Wednesday, October 21, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Wednesday, October 21, 2026

● (1630)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): We will now call the meeting to order.

Good morning, everyone. Thank you for joining us in person or virtually to take part in meeting number 51 of the House of Commons Standing Committee on Public Safety and National Security.

Pursuant to Standing Order 108(2), we are meeting today to review Canada's security screening process, pursuant to the motion adopted on August 17.

I'd first like to welcome the three witnesses, all of whom are participating in the meeting remotely.

We welcome, as individuals, Christian Leuprecht, professor at the Royal Military College of Canada, and Michael Wernick, Jarislowsky chair in public sector management at the University of Ottawa. From the Canadian Space Agency, we have Jean-Claude Piedboeuf, senior vice-president, space programs.

Each witness will have five minutes for their opening remarks.

Mr. Leuprecht, you have the floor

Dr. Christian Leuprecht (Professor, Royal Military College of Canada, As an Individual): Good day, ladies and gentlemen.

Mr. Chair, thank you for your comments and the invitation.

I'll be speaking in English and I'll respond to your questions in either official language.

[*English*]

I have spent two decades researching and writing on matters of national security, including matters of research security, with which I am particularly familiar. I have also written a book on the Five Eyes intelligence community. As a professor at the Royal Military College who collaborates with other government departments, I'm also subject to security screening processes.

The system will never get it perfect every time. Rather, the system is meant to make reasonable assessments on risk on the front end relative to the person, position and tasks, and subsequently it needs to be agile and dynamic when flags arise. The case that triggered today's meeting is indicative of failures on both ends: a failure to assess risk appropriately on the front end, and a subsequent failure to act on weak signals.

I offer three observations to that effect.

In February of this year, the Jamestown Foundation released a report that pegged Canada as the most subverted by China among G7 countries. The foreign interference commission documented the scope and scale of foreign interference and malign influence in Canada, especially by China's United Front Work Department. In 2024, the National Security and Intelligence Committee of Parliamentarians finally released the redacted version of its long-awaited report on foreign interference in Canada's democratic processes and institutions.

Sam Cooper has documented the extent of elite capture among Canada's political, diplomatic, business and corporate networks at the federal, regional and local levels. The scope, scale and sophistication of adversarial activity against Canada is well documented in the unclassified versions of CSIS's annual reports. In other words, the government would have been well aware of the risks and vulnerabilities emanating first and foremost from China.

Between 2020 and 2023, the government effectively tripled the immigration intake to nearly two million immigrants. No commensurate additional resources were provided to the three agencies in charge of vetting new entrants to the country: CBSA, IRCC and CSIS. We can infer that tens if not hundreds of thousands of people were allowed to enter and reside in the country without having undergone proper vetting. Similarly, between 2015 and 2024, the civil service grew by over 40%, from 257,000 to 368,000 employees, but with few additional resources for the security and intelligence community, many are unlikely to have been scrutinized thoroughly.

Immigration levels, the size of the civil service and the allocation of resources are ultimately political decisions. The government of the day opted to prioritize immigration and growing the civil service over security and vetting. In other words, the government knowingly exposed Canada and the civil service to heightened security risk. The infamous case of the government awarding an X-ray contract for Canadian embassies to Nuctech is a case in point. The federal government's half-hearted research security policy is another example. The federal government needs to strike a better balance between its policies for growing immigration and the civil service on the one hand and ensuring the integrity of technology and of people admitted to stay in the country and hired as civil servants on the other.

Foreign spies know they can operate in Canada with relative impunity. The two Chinese scientists at the level four microbiology lab in Winnipeg were somehow able to leave the country during COVID, when travel was highly restricted, rather than face justice, and the government actively suppressed related documentation. Russian GRU officer Mikhail Mikushin was able to study and operate unimpeded in Canada until he was picked up by authorities in Norway. In the case that triggered this hearing, which is a classic problem of weak signals, the target ran afoul of federal policy, but the primacy of EDI policies has a definitive chilling effect on any manager taking the risk of flagging the reliability of a young, racialized woman.

In short, this is not, first and foremost, a failure of the security screening processes. The government has been well aware of the risk posed by China. The government opted not to optimize resources commensurate with the scope and scale of the threat. When risks do arise, the government prefers to make problems go away over taking action to protect the security of the country and allies. It's hard to overstate the reputational damage when foreign spies operate in Canada but are then picked up by our allies.

Ultimately, this is not a failure of the security screening process. It is a failure of political will to recognize and act on foreign threats to the national interest and national security, which is exacerbated by an institutional culture that disincentivizes acting on weak signals [*Technical difficulty—Editor*]. The take-away is the need for political will to realize that subversion and insider threats in federal institutions—

● (1635)

The Chair: I'm sorry, Mr. Leuprecht. We'll pause for a few seconds to make sure that the interpreters can hear you well. I believe there are communication difficulties.

Can you start again?

Dr. Christian Leuprecht: [*Technical difficulty—Editor*]

The Chair: That's unfortunate. I have to stop the intervention, because we cannot understand.

While we try to fix your connection, Mr. Leuprecht, let me turn to Mr. Wernick for five minutes, and then Mr. Piedboeuf. We may be able to come back to you for the last minute at the end of Mr. Piedboeuf's intervention.

Mr. Wernick, go ahead.

[*Translation*]

Michael Wernick (Jarislowsky Chair in Public Sector Management, University of Ottawa, As an Individual): Thank you for the invitation.

I'm curious to know why I was invited.

[*English*]

I have no opening statement for you. I'm happy to take questions and try to assist the committee. I've been invited often to parliamentary committees, and I respect the work that you do.

I should just clarify for members, especially the newer ones, that I left the government seven and a half years ago. I no longer have a security clearance. It's been years since I went through one. I have no contact with the people in the government you were examining last week. I haven't spoken to anybody in the government about this issue, and I have no particular knowledge of the case other than what I've read in the open media.

I may be able to help you with some sense of where the weaknesses in the current system lie and perhaps around issues of accountability and machinery of government in terms of moving forward to improve the system.

● (1640)

[*Translation*]

The Chair: Thank you, Mr. Wernick.

Mr. Piedboeuf for five minutes.

Jean-Claude Piedboeuf (Senior Vice-President, Space Programs, Canadian Space Agency): Thank you, Mr. Chair.

My name is Jean-Claude Piedboeuf, and I'm senior vice-president, space programs, at the Canadian Space Agency. Thank you for the opportunity to appear before the committee to present the Canadian Space Agency's approach and posture to security, as well as measures we are taking to strengthen it.

I understand that the committee may be interested in the incident in Belgium, but because of the ongoing investigation, I'll limit my observations to Canadian Space Agency's security screening, control, information sharing and surveillance mechanisms.

[*English*]

The mandate of the Canadian Space Agency is to promote the peaceful use and development of space, to advance the knowledge of space through science and to ensure that space science and technology provide social and economic benefits for Canadians. Our mandate is based on innovation and collaboration. It also requires us to protect the people, information, facilities and technology entrusted to us by ensuring the rigorous management of space programs and missions, which often involve advanced technologies, sensitive scientific information and specialized facilities.

These activities are carried out in collaboration with government, industry, academia and international partners. In this context, security screening helps protect sensitive information, assets and activities of the Government of Canada. Depending on the nature of the duties and the access required, the individuals concerned must have the appropriate security status or clearance.

Security screening at the CSA is conducted within the framework established by the policy on government security and the TBS directive on security screening. These instruments establish the government-wide framework applicable to security screening. The deputy head designates a chief security officer, who exercises the responsibilities and authorities assigned to them for security screening.

[*Translation*]

Security screening is an essential component of our approach. It helps assess individuals' reliability and their eligibility for the access information required to perform their duties. A security clearance doesn't automatically provide access to all information at the same level. Access is granted based on the person's responsibilities in compliance with the need-to-know principle.

More specifically, when an employee requires access to protected information, the minimum security level they require is reliability status. At the Canadian Space Agency, most positions require either reliability status or a secret security clearance. A smaller number of functions require a top secret security clearance.

The required level is determined according to the position, including the duties to be performed and the sensitivity of the information, assets, facilities and systems to which the individual requires access.

The Canadian Space Agency applies a structured security screening process that includes the individual's consent, verification of their identity and background, and any other checks required for the screening level. In addition, Internet searches are conducted as needed when adverse information is identified in a security file. The Internet search program for top secret clearances is expected to be launched in November 2026.

[*English*]

As part of this process, the CSA engages the appropriate federal partners when required, including the RCMP and CSIS, in accordance with their respective responsibilities. The full results of these background checks are assessed before a decision is made by the chief security officer and the authorized delegated officials, in accordance with the delegation of security screening authorities.

In recent years, the CSA has added security resources to strengthen its capacity. The agency has also increased the number of individuals holding top secret security clearances, delivered space security awareness sessions and conducted threat and risk assessments. It will continue to strengthen its security posture as threats and risks evolve to ensure that sensitive Government of Canada and partner information is managed according to rigorous standards tailored to security requirements.

The CSA maintains continuous monitoring by combining automated mechanisms, periodic controls and the tracking of security events. The CSA monitors cybersecurity alerts and access, improves physical security systems and monitors changes that could alter the level of risk. Incidents and information of concern are assessed and followed up with appropriate measures.

● (1645)

[*Translation*]

In conclusion, effective security screening is essential to protecting the sensitive work entrusted to the Canadian Space Agency. At the Agency, we place great importance on protecting our information, facilities and people, and on maintaining a strong security culture. We'll continue to rigorously apply government security screening requirements and work with our partners to protect the activities and information entrusted to us.

Thank you for the opportunity to appear before you today. I would be pleased to answer the committee's questions.

The Chair: Thank you very much, Mr. Piedboeuf.

[*English*]

Mr. Leuprecht, would you like to try to conclude your intervention? You have a minute and a half left.

Dr. Christian Leuprecht: Mr. Chair, where would you like me to pick up for the interpreters?

The Chair: Anywhere you would like, given that you have one minute and a half left.

Dr. Christian Leuprecht: I'll just repeat my concluding paragraph.

In short, this is not, first and foremost, a failure of the security screening process. The government has been well aware of the risk posed by China. The government opted not to optimize resources commensurate with the scope and scale of the threat. When risks do arise, the government prefers to make problems go away over taking action to protect the security of the country and allies.

It is hard to overstate the reputational damage when foreign spies operate in Canada but are then picked up by our allies. Ultimately, this is not a failure of the security screening process. It's a failure of political will to recognize and act on foreign threats to the national interest and national security, which is exacerbated by an institutional culture that disincentivizes acting on weak signals of potential insider threats.

These are the take-aways: We need political will. We need to realize that subversion and insider threats in federal institutions are pervasive. We need to resource the security and intelligence community accordingly, and we need to hold managers to account.

The committee may want to ask this question: Have any managers, deputy ministers or ministers been held to account in this or other cases of insider threat in the Government of Canada? Focusing on the security screening process is to miss the forest for the trees.

[*Translation*]

Thank you.

The Chair: I sincerely thank all three witnesses for their much-appreciated opening remarks. We will now move to questions from members.

Ms. Kirkland for six minutes.

[*English*]

Rhonda Kirkland (Oshawa, CPC): Thank you, Chair.

Thank you to our witnesses for appearing today. I appreciate the time you are giving us.

I don't know if you have followed this committee's study on this specifically, but by way of review, in a previous committee meeting, a Global Affairs Canada official confirmed something that I found pretty concerning. I asked the question in a very broad way. It's been repeated today that we're not going to dig into something that is under investigation in Belgium. However, we did find out that if an individual were found to have committed fraud in a federal hiring process, that finding would not automatically be flagged in future security screenings if they were never hired or granted a clearance.

We now have a Canadian, for instance, which is why we're doing this study, who was found to have committed fraud in a federal hiring process. She obtained an internship at NATO. That much we know. We know that she's facing serious espionage allegations in Belgium.

Mr. Wernick, I appreciate your being here today and your being open to questions. I'm hoping to glean something from your experience as a former top public servant.

Does it concern you that someone could be found to have committed fraud in one federal hiring process, yet that information might never reach officials responsible for their next security screening?

Michael Wernick: It's a great problem. It's a terrible weakness in the screening process, and it's an issue in other matters of personnel. I've written and spoken about this in other contexts.

There is a gap between the security perspective.... What the agencies are going to be looking for in a security clearance tends to focus on vulnerability to blackmail, vulnerability of foreign influence, criminal contact, drug and alcohol dependency, suspicious contacts, extended family and business and so on. Those are relatively straightforward methodologies for the RCMP, CSIS and the other agencies.

One of the other criteria, though, in terms of being trustworthy and loyal, is personal conduct. There's a whole set of other issues around personal conduct, misconduct and wrongdoing by public servants and others that isn't systematically collected across the public service. These are things that I think have come up in some of these cases: misrepresentation of credentials, workplace conduct, harassment, bullying, sexual harassment, cheating on tests and all that sort of thing.

There is no single repository for that. It is possible for somebody to escape consequences by moving from one department or one agency to another. There are almost 300 federal agencies in the core public service. You can look them all up on GC InfoBase.

I think the time has come for the Treasury Board of Canada Secretariat to force the creation of some kind of central repository—I'm not sure what the right terminology would be—a clearinghouse, a place where all of the information related to.... Well, I think you'd probably want to have it in two parts. The secure part is information that's clearly related to security clearances and that can be moved around the community across departmental security officers, but you don't want to flood it with the other part, I think, which is going to be all of the disciplinary actions, substantiated transgressions, findings by the various watchdogs and so on.

They're not—

● (1650)

Rhonda Kirkland: I'm sorry to interrupt—

Michael Wernick: —systematically collected in one place, and they should be.

Rhonda Kirkland: Okay. That's exactly what I wanted to get to.

I agree. It doesn't have to sort of be everything, but when someone commits fraud, it would seem to me that it should be an automatic red flag. All the names they've ever used, including their real name, should be in some sort of database that tells anyone else who is hiring across the public service that this person has done something that we would definitely consider untrustworthy and is someone who should perhaps not have such a great security clearance as they would have with NATO.

In your experience, then, who should be responsible for ensuring that a substantial finding of fraud follows an individual through the subsequent federal hiring and security process? Ultimately, who's responsible for making sure that this gets fixed for the future?

Michael Wernick: The President of the Treasury Board and the Treasury Board of Canada Secretariat: The closest thing we have to a management board or a chief operating officer in the Government of Canada—and it's not fully functional—is the President of the Treasury Board. They have all of the tools for financial management, human resources management, information management and language policies and, as you saw, they issue the directives on security clearances.

Rhonda Kirkland: How do we make them—

Michael Wernick: They have the leverage. One of the things you could recommend is that the government adopt an unambiguous “one public service” model for security clearances—we're very close to that on cybersecurity—and that the President of the Treasury Board report to you every six months on what they have done to close gaps and seams and get rid of stovepipes.

Rhonda Kirkland: I think that's a great idea, but ultimately, the public safety department.... The President of the Treasury Board, for sure...but which minister, then, is ultimately responsible to make sure the President of the Treasury Board—

Michael Wernick: The President of the Treasury Board is the chief operating officer—

The Chair: I'm sorry to interrupt, Mr. Wernick. We often have great questions in this committee but not often the time to have the great answers that are expected. We may get back to it later.

We turn now to MP Sodhi.

Ms. Sodhi, you have six minutes, please.

Amandeep Sodhi (Brampton Centre, Lib.): Thank you, Mr. Chair, colleagues and all of our witnesses for being here today.

I would like to begin with you, Dr. Leuprecht.

As you know, a thorough security assessment requires more than just collecting information from an applicant. Departments also need to determine whether that information is complete, accurate and sufficient enough to support a reliable decision, which they make. Are there particular checks or verification measures that you believe the government should strengthen to ensure potential security concerns are identified before a security clearance is granted?

● (1655)

Dr. Christian Leuprecht: There are two separate problems here. The first is how we deal with insider threats. What we have here is a definitive problem of an insider threat. People may be entirely admissible in terms of getting enhanced reliability, secret or TS clearance, and then engage in behaviour that is fundamentally intended to subvert the conditions under which they were hired in terms of reliability. One question is this: How do we pick up insider threats? The other is this: How do we pick up individuals whose conduct is clearly intended to deceive and to subvert the process in place to get hired into the government to begin with?

This is not just a government problem. Just today, I spent time with some of the representatives from the Canadian banks. They also have no effective mechanism to prevent someone who engages in improper behaviour in one bank from walking across the street and doing it in the bank across the street. This is not just a government problem. This is a Canadian problem.

The Privacy Act is up for review. One of the elements here is that we need a more robust legislative framework in terms of effective sharing of private information both within the government and among key critical infrastructure institutions in this country.

The other is to ensure that this information is acted upon. In this particular case, the government and the manager would have had the option of an administrative investigation. If that administrative investigation had found...to be fraudulent—the former clerk can correct me on this—that would have been grounds for this individual to be dismissed from the ability to be employed in the federal civil service.

What it suggests to me is that the tools at the disposal of the manager were not utilized to the full extent. I believe I outlined in my statement why that is; it's because there's a disincentive and a chilling effect for managers to act on such information. It is notoriously easier to make the problem go away than to take responsibility.

Amandeep Sodhi: Thank you for your answer.

Mr. Wernick, you have previously proposed creating a single registry that tracks findings of misconduct or mismanagement identified by oversight bodies and that allows relevant information to follow employees between departments. This could help prevent important information from being overlooked when an individual changes roles.

What would this registry look like in practice, and how could the government ensure that relevant findings are recorded, verified and appropriately considered during the security screening process?

Michael Wernick: You're going to take me beyond my technological ability. It does seem to me that it's a relatively straightforward piece of software.

You'd also want a similar system for contractors. We're talking about roughly 300,000 employees. However—and I think I'm seeing some heads nodding—there's significant risk with contractors and the employees of contractors, who are often engaged in very delicate procurements, defence installations and so on.

It does occur to me—again, I'm not an expert—that this is tailor-made for AI, for AI to examine large databases, put up flags and make patterns and connections.

We need to catch up on the basic accountability. The government should be publishing at least once a year some kind of report on the security clearance process of personnel and contractors: how many, what level, the timeliness and the organization. That's the basic mechanism by which accountability works. It's not a perfect model.

The pillars of the Canadian model of accountability are the deputy heads and heads of agencies. They have a lot of authority given to them, but they're also accountable under about 40 different statutes—the Financial Administration Act, the Federal Accountability Act, the human resources act and so on. They are guided and corralled by Treasury Board policies, and they are overseen by about 14 watchdogs.

That model works most of the time, but it doesn't always work. I think in this case we need a stronger Treasury Board to intervene on this. We need more modern 21st-century information sharing to prevent this problem of people migrating from one part of the service to another.

I would also add, before the chair cuts me off, that the problem extends to other federal agencies that are critical to democracy. You need to look at Elections Canada, the network of returning officers, courts administration, the people who work for Parliament and the people who work for our officers of Parliament. We need a consistent approach to personnel and contractor screening, just like we do with cybersecurity.

● (1700)

[*Translation*]

The Chair: Thank you very much.

Mrs. DeBellefeuille for six minutes.

Claude DeBellefeuille (Vallée-du-Haut-Saint-Laurent, BQ): Thank you very much.

I want to thank the witnesses for joining us.

Mr. Wernick, I was taken aback during your remarks earlier when you said you didn't know why you were here and were curious why we invited you.

I came across an article published in the Ottawa Citizen in August, in which you were reacting to Ms. Zhang's case. You said that one of the reasons the process failed was because it had long been under-resourced.

Do you stand by this comment you made to the Ottawa Citizen in August?

Michael Wernick: Yes.

Claude DeBellefeuille: Okay.

You're talking about funding, but we know that funding increases are not necessarily the way to always achieve our objectives.

In your terms—as someone with extensive experience in government administration—what does additional funding mean? What adjustments are needed? What would need to be added so that we can implement better measures, be better equipped to conduct security screenings, and prevent what happened this summer?

Michael Wernick: I think it would be a combination of the number of employees assigned to this role, technology, meaning the platform and the software—I mentioned the possibility of improving that—and training. It would be a mix of those three things.

Claude DeBellefeuille: You agree to some extent with Mr. Leuprecht, who says that, ultimately, this isn't just a matter of process but also a matter of political will: If policy makers decided to take this issue seriously, they would allocate the necessary resources and do everything in their power to prevent such a situation, even though we know that there's no such thing as zero risk.

What I understand then is that if there were political will and additional resources, and if the problem were truly taken seriously, perhaps we could build a more robust process to counter the espionage we're facing. I was surprised to learn that Canada is the country most heavily infiltrated by China worldwide. Consequently, we need that robustness.

Given your extensive experience, how do you explain this lack of political will to allocate additional resources in 2026, considering everything we now know about the espionage Canada is facing from China or other countries?

Michael Wernick: Since I left the public service a long time ago, all I can say is that every budget, every year, comes down to priorities. Another budget will be tabled in a few weeks, and the finance minister must deal with pressure from all sides, including in relation to the topic we're discussing today.

Claude DeBellefeuille: I think your testimony is more than credible. Based on what you're saying, in the next budget, given the current state of espionage against Canada, we could expect increased resources for security screening to ensure it's stronger and better protects government, its corporations and agencies.

Michael Wernick: Yes, absolutely. The committee could make this recommendation to government colleagues and the finance minister, who is in the last few weeks of preparations for the next budget.

Claude DeBellefeuille: The foreign influence transparency commissioner could also make a recommendation; we have not yet had the privilege of welcoming him to our committee. Perhaps he made this recommendation to the government too.

As a former senior official, you know that public servants are unionized. They have a collective bargaining agreement. However, I sometimes get the impression that collective bargaining agreements do not allow the sharing of human resources data or the creation of a central human resources registry.

Can you tell me whether I'm off base or whether my concerns are justified?

● (1705)

Michael Wernick: I don't know if collective bargaining agreements contain such provisions.

What matters is the legislative framework. And it's you, the members of Parliament, who control the legislative framework. As for striking a balance between privacy protections and security needs, it's your responsibility, as parliamentarians, to find the right balance.

Claude DeBellefeuille: It's important to understand that the Public Service Commission explained to us that creating a registry isn't that simple, since there's not only the issue of collective agreements, but also the issue of the right to some protection. For example, if someone commits fraud, it can remain on their record for two or three years, and then it is expunged.

How far do you think we can go with this registry?

Michael Wernick: I think these are just excuses. Espionage and interference are quite serious matters. We need to act now and create something that is, obviously, very secure: We don't want to create a database that could become a target.

However, I think we can identify protective measures and remedies. We could certainly introduce a bill quickly that this committee could study in order to strike a balance, as we do in other areas.

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

[*English*]

Mr. Lloyd, go ahead.

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

Thank you to the witnesses.

I'll start with Mr. Wernick. In your time in the civil service at the highest levels, did you have any concerns about the infiltration of the civil service or contractors of the Government of Canada by organized crime elements or elements of foreign interference?

Michael Wernick: There's always a general concern, and you want to make sure that there are systems of protection and screening in place. I can recall only a few specific cases coming up when I was the deputy minister at Indian Affairs or at the Privy Council. They were dealt with on the advice of the national security adviser and the departmental security officers.

Dane Lloyd: What was the process that brought those cases to the attention of authorities?

Michael Wernick: There were intelligence briefings.

Dane Lloyd: From whom?

Michael Wernick: It would depend. There's a departmental security officer for every department. Then, when I was a PCO, which was my last gig, it would have been the national security intelligence.... What was it called?

Dane Lloyd: Without getting into the specifics of any case, what did you usually find was the trigger for these investigations?

Michael Wernick: Every case would be different. It's usually about the contacts of the person with foreign governments, foreign entities. Those are the sorts of things that I recall coming up.

Dane Lloyd: Thank you.

I'm going to go to Professor Leuprecht. You talked about political failure. I've been in this role, and I've heard from witnesses saying that there is an issue, that organized crime elements are infiltrating the government for the purpose of passing information that might be useful for criminal elements. I know there were allegations related to auto theft, that information was being passed from driver's registrations to organized crime in order to facilitate the theft of vehicles.

Can you tell us what things we should be watching for in the civil service?

Dr. Christian Leuprecht: Without prejudice to my colleague, during his tenure we had the most colossal recent failure of security screening in this country, which was the arrest of the director general of criminal intelligence for the RCMP, Cameron Ortis, who was found guilty of very serious charges.

We have a pattern here of people engaging in insider threat activity, and we have a challenge that I think the government is not postured for: The policies are not designed for it and the responsibilities with regard to managers are not in place. If we're not looking for it, we're not going to find it.

What we have is much like what we often have in government. We have a spreadsheet, a checkbox process: “I've checked all the boxes, so as a manager, I'm okay because I've done my due diligence.” I think what we need here is a consequential change in institutional culture, given that Canada is living in a very volatile environment in which it has never been more important to protect the national interest and national sovereignty from malign elements that are looking to divide, undermine and subvert us.

● (1710)

Dane Lloyd: Thank you.

You know, I think that in many ways, when we talk about these cases, we focus on the intake. We want to build high walls to keep threat actors out from positions of influence. However, what's being done for people who are already...? They might not be compromised. They might already be working in areas, and then they become compromised later on. What can we do to protect from within?

Dr. Christian Leuprecht: Mr. Wernick alluded to what we do on cyber. On cyber we've long abandoned the castle model, the idea that we can somehow have big walls and keep the adversary out. We know that the adversary is inside the castle, yet it seems the security screening process still operates on the idea that somehow we can build a wall that's big enough and tall enough to keep the adversary out.

I would say that we need to adopt precisely the cyber approach we have. We have to assume now that we have enough evidence that the adversary is inside the castle, so we need to make sure we have the processes in place to identify those risks, to be able to act on those risks in a timely and effective manner, and to make sure that information and intelligence is shared effectively. What we have is a regime that is good at reporting, but the regime is very poor at turning reporting into actionable intelligence and sharing that intelligence across the federal civil service.

Dane Lloyd: Do you think the—

Michael Wernick: Perhaps I can add this. I think it will be helpful. These are not lifetime passes. They're time-limited. When people change jobs or move into a job with a different information requirement—

Dane Lloyd: Thank you.

Michael Wernick: —their clearances can be upgraded, downgraded or revoked.

Dane Lloyd: Yes. Thank you. I appreciate that.

I—

The Chair: I'm sorry, MP Lloyd.

Dane Lloyd: He took my time.

The Chair: I suspect that you have many more things to add. Hopefully, that will be possible later.

[*Translation*]

Ms. Dandurand for five minutes.

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

I thank the witnesses for joining us.

Mr. Wernick, I'd like to give you the opportunity to complete the thought you were expressing.

Michael Wernick: Which one was that?

Marianne Dandurand: The one you were just talking about, in relation to the process.

Michael Wernick: I just wanted to say that these clearances aren't permanent. They have to be renewed every five or ten years, depending on the level. If you change jobs or if circumstances change such that you need more or less access to classified information, there is a whole process for granting and revoking the security clearance, as well as for raising or lowering the security level.

I think it would be a good idea for the government to publish, at least for one year, the figures on the volume of these operations.

[*English*]

I think it would be very good if the government provided to NSICOP a classified briefing on how many cases of security clearances were rejected, downgraded or revoked. They would get a sense of the pattern. They would get a sense of where there might be some vulnerabilities.

[*Translation*]

Marianne Dandurand: Thank you very much.

You were a long-time public servant. You were also responsible for Treasury Board, which is in large part responsible for—

Michael Wernick: No.

Marianne Dandurand: No? Pardon me.

You were a long-time public servant, where you were responsible for similar initiatives.

In your opinion, at what point should the security screening process be centralized? At what point should it fall under a centralized agency rather than under each department? We have been having this discussion since this study began. How much liberty should each department get in this regard?

Michael Wernick: I think it will always be a combination of the two. It's a balance. Investigative expertise lies with the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and other security and intelligence agencies. These organizations have the training and expertise to conduct vetting. However, I believe agency leaders have a better understanding of the context within their own institutions. The Canadian Coast Guard is not the same as a science lab, for example. This dialogue between the two works well.

What's sometimes missing is an ad hoc exchange of information. I think we need more centralization and more consistency. I'm thinking in particular of an electronic database that would bring together all federal organizations. It's time to do this.

There's a problem in the public service. It's a kind of “not in my backyard” syndrome. Agencies think they're special and want to do things their own way. I've always been in favour of a model where the central government—especially Treasury Board—would take on more of a leadership role toward other agencies and departments.

● (1715)

Marianne Dandurand: I'm curious to hear your opinion on the level of accountability of the government compared to that of the public service. I get the impression that broad guidelines probably need to come from policy-makers, but that agencies must then use their own judgment to implement them.

From your perspective, should government guidelines be stricter, or is the administration able to ensure security under the current rules?

Michael Wernick: I can't comment in detail. I know the Treasury Board policy was updated two years ago, I believe, and that a Treasury Board representative testified last week. He was asked that question.

I believe this type of Treasury Board policy is always subject to a review and renewal process. These policies have a term of three, four or five years, after which they are renewed. They stem from decisions made by a cabinet committee. They are very official. They are guidelines that other agencies and departments must follow. There are consequences if they are not followed.

The Chair: Thank you very much, Mr. Chair.

Mrs. DeBellefeuille for two and a half minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Mr. Leuprecht, in your speech, you said there was an institutional culture that prevented people from pointing out weaknesses in the process or from being on the lookout for warning signs. What did you mean by that? I'd like you to take two minutes to explain it to us in concrete terms.

Dr. Christian Leuprecht: Yes, ma'am. That's a very good question.

I'd just like to correct something regarding the report you mentioned. Canada is the G7 country most heavily infiltrated by China.

Basically, Canada takes a rather homeopathic approach to national security, including national security issues within the government. In the case at hand, we had a problem with weak signals in particular. Now, we need to hold managers accountable.

Let me give you the example of sexual harassment in the public service. For example, within the armed forces, ample evidence has shown that the easiest way to get rid of someone who engaged in unacceptable conduct was to reassign them to another position or even promote them so that the unit would no longer have that problem. However, the armed forces have now completely changed their approach. Managers are now held accountable for the conduct of the people under their supervision. This is the approach that must be adopted throughout the public service.

The problem is that we've created a culture where managers no longer take responsibility for their work or their employees. Instead of making difficult decisions, they pass those difficult decisions up the chain of command.

Claude DeBellefeuille: In this example, when it comes to security, where did the failure in the line of accountability occur, in your opinion?

Dr. Christian Leuprecht: I think it would be interesting for the committee to find out who in the public service was held accountable for the conduct of the individual at the centre of today's discussion.

I believe that probably no one in the public service has truly taken responsibility for the fact that someone actually attempted to commit fraud. Instead, people said it wasn't that serious and the matter was dropped. This was done for the reasons I explained—namely, that diversity policies, which are, in principle, good policies, deterred managers from taking action against a young woman of colour.

● (1720)

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Lloyd for five minutes.

[*English*]

Dane Lloyd: I'll be brief.

This is for Professor Leuprecht and Mr. Wernick. I'm trying to be systematic.

Is the Public Prosecution Service of Canada equipped to deal with these national security cases? Does it have what it needs? Does it have the expertise?

Finally, in cases of these investigations and these trials, do you feel it's too secretive, or do you find that level of secrecy is warranted, based on the cases?

Thank you.

Dr. Christian Leuprecht: I think we need to separate—and the former clerk can correct me on this—criminal processes from disciplinary processes. There is a host of disciplinary options available to managers, depending on the sort of infraction on which there are reasonable grounds to believe an employee may have committed, and those usually start with a type of investigation. The type of investigation is a function of the infraction that is suspected, and those investigations can include up to dismissal of the employee.

At that point, when an investigation is launched, there is then opportunity to ascertain if the investigation finds that there's criminal behaviour or, at the beginning, a suspicion of criminal behaviour. Either the investigation is pushed to the RCMP for criminal investigation, with the involvement of the PPSC.... We've learned from past mistakes that we need to bring in the PPSC much earlier, but of course the investigation would be run by the RCMP in coordination with the PPSC.

The investigation would not be pushed to the PPSC per se, but there is probably a question about how early and under what circumstances we should ensure that criminal investigations are initiated, so that the evidence is collected successfully. I worry that in the process before us, for instance, if there would have been suspicion of criminal conduct, we might have not run the investigation in a way such that the evidence would have subsequently been admissible for a criminal proceeding.

Dane Lloyd: Mr. Wernick.

Michael Wernick: I don't have much to add in terms of PPSC. I know that their resources are adjusted when there are new laws they have to deal with. Another committee is studying the financial crimes agency bill, which will affect the workload of PPSC, so they will have a dialogue with the Minister of Finance about their resourcing.

I would say that there are two recurrent problems.

We had a lot of issues with contractors when I was a deputy minister at aboriginal affairs and in many cases referred issues to the RCMP to look into potential fraud. It would often take two to three years before anything would come back, and they would often abandon the case because it was just too damn hard to collect any kind of evidence. The deputy is left with "what do I do with this contractor or this employee under investigation?" when it's going to take that long.

I don't have any solutions for you in terms of how to speed up these investigation processes. Sometimes they result in a finding that, no, there was nothing there. You have to be careful with the set points on this.

I would just make one other point that the committee may not be aware of, which is that if a job requires top secret clearance or secret clearance, and you revoke the security clearance, you've effectively fired the person.

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you. I'll pick up there.

Mr. Piedboeuf, could you please tell us...? You said you could not comment because an investigation was under way. What investigation is under way?

[*Translation*]

Jean-Claude Piedboeuf: I was referring to the incident in Belgium.

[*English*]

Frank Caputo: I understand that the investigation in Belgium is under way, but who is undertaking the investigation that prohibits you from commenting?

[*Translation*]

Jean-Claude Piedboeuf: I can't comment on the case.

[*English*]

Frank Caputo: Okay. It's Belgium. There is no investigation by your agency at this time.

Jean-Claude Piedboeuf: No, we cannot comment on a case that is under investigation by Belgium.

● (1725)

Frank Caputo: I understand. I'm not asking for you to comment.

I want to be very clear. What I'm asking is whether your agency is not investigating somebody that is alleged to have been a spy that worked for your agency. Doesn't it follow that your agency would be doing an investigation of its own?

[*Translation*]

Jean-Claude Piedboeuf: Unfortunately, I can't comment on the case because it's under investigation.

[*English*]

Michael Wernick: No, not at all. Once you turn it over to the police, you cannot continue an investigation because you may compromise the police investigation.

Frank Caputo: With all due respect, I wasn't asking whether the police have been contacted or anything like that. I was asking the head of the Canadian Space Agency whether they are doing an investigation internally as to what happened, because somebody who worked for them went on to be alleged to be spying for China.

Is there an investigation into what happened at the Space Agency? Just a yes or no, please....

[*Translation*]

Jean-Claude Piedboeuf: Unfortunately, I can't comment on the case because it's under investigation.

[*English*]

Frank Caputo: No, but—

The Chair: I'm sorry, MP Caputo. I always regret doing this, but we now need to move to MP Powlowski for five minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Far be it for me to be defending our bureaucracy. On several occasions, I've been critical of our own bureaucracy. However, you made some quite inflammatory statements about our bureaucracy. I wonder whether you can substantiate them.

Correct me if I'm wrong, because as you were saying it, I was trying to take notes. You said that between 2015 and 2024, there was a 40% growth in the civil service. You said that many of those people were “unlikely” to have been screened. Do you have proof that they weren't actually screened?

The second thing you said—and correct me if I misquote you—is that the bureaucracy “knowingly exposed” the country to risk. Again, that's a fairly extreme statement. You said “knowingly”. Do you have any proof, really, that the bureaucrats knowingly exposed the country to risk?

Dr. Christian Leuprecht: First, let's start with my colleague from the Canadian Space Agency. This is, of course, the second case for the Canadian Space Agency.

Mr. Wanping Zheng was subsequently found not guilty, I should admit. Of course, there appears to be, just in his example, a pattern of an insider challenge.

Marcus Powlowski: Hold on. One case does not constitute an example. It is an example, I guess, but it doesn't constitute—

Dr. Christian Leuprecht: That's why I made the point that there's been at least a second case in recent years.

What I did point out is that the screening was not conducted at the levels and commensurately, as would have been necessary and appropriate. The inference I draw is that the amount of growth for the civil service was not commensurate with the resources that were allocated to the entities that are ultimately tasked with doing a closer vetting when somebody does end up being triggered.

I didn't say that people didn't get screened. I pointed out that the resources were not commensurate.

I didn't say that the bureaucracy “knowingly exposed” the country. You'll have my written statement, which I've provided to the clerk. I said that political decisions were made to not allocate the resources that would have been appropriate, given both the growth in the civil service and the well-known vulnerabilities of this country, particularly to a very aggressive and sophisticated adversarial actor, that being China.

Marcus Powlowski: You're denying now that you said that the bureaucracy “knowingly exposed” the country to risk. Are you retracting that?

Dr. Christian Leuprecht: You have my written statement in front of you, and I read from my statement.

I can find the line, but the essence is that the bureaucracy was knowingly exposed to risk by political decisions. Commensurate security resources were not provided to ensure that the screening for 50% more civil servants could be done thoroughly for cases where more in-depth screening would be necessary.

I can say with a reasonably high degree of certainty that there are likely cases where decisions simply would have been made about whether to “just let this one go” or not, given the relative growth.

I've been on record for years as saying that Canada, both with regard to its federal bureaucracy and with regard to the country, has a rather homeopathic approach when it comes to national security. I think the multiple reports that I cite in my statement document that, particularly when it comes to China.

● (1730)

Marcus Powlowski: Okay. I want you to clarify something else.

Again, correct me if I'm wrong, but you said with respect to Ms. Zhang that there was a security lapse in not flagging the vulnerability “of a young, racialized woman”. Are you implying or telling us that people of racial minorities are more likely to be treasonous or should be subject to a higher degree of scrutiny?

Dr. Christian Leuprecht: That is neither what I said nor the inference to be drawn.

What I pointed out is that in a federal government that has made it clear that it prioritizes diversity policies, a manager—particularly a junior manager—who would be flagging such an individual had better come with very robust evidence or likely face serious headwinds in trying to flag that individual.

What I'm saying is that we need to create an environment where even weak signals can be taken seriously and reported by managers without fear of retribution when the individual involved in weak signals might be an individual whom government priority and government policies have favoured.

Marcus Powlowski: Is being a minority a weak signal of risk?

The Chair: I'm sorry, MP Powlowski. Again, I hate to do this, but time is up.

[*Translation*]

Now is the time to thank the three witnesses for taking the time to be with us, for making the effort to prepare, and for attending today's meeting.

Mr. Leuprecht, Mr. Wernick, and Mr. Piedboeuf, we'd like to express our gratitude to you, and we hope you enjoy the rest of your day.

I now turn to the members of the committee. We will recess for five minutes before resuming with three more witnesses.

Thank you.

● (1730)

_____(Pause)_____

● (1735)

The Chair: We are resuming our meeting.

Thank you for joining us for the second hour of this meeting, for which we have three witnesses.

We welcome Dr. Wesley Wark, senior fellow at the Centre for International Governance Innovation, appearing as an individual. From Cinchy Incorporated, we welcome J. Paul Haynes, chief executive officer. Finally, from the Privy Council Office, we welcome David Morrison, senior diplomatic and international affairs adviser to the Prime Minister.

You each have five minutes to present your remarks.

We will begin with Dr. Wark.

● (1740)

[*English*]

Dr. Wesley Wark (Senior Fellow, Centre for International Governance Innovation, As an Individual): I thank you, Chair and members of the committee, for this invitation to appear as part of your study on Canada's security screening processes.

I'm going to take you in a different direction and scare you, perhaps, in a different way than you've heard from your witnesses in the previous session. I want to begin by making a few factual points.

The Government of Canada process for security screening is set out in detail in a relatively new directive on security screening that only came into effect on January 6, 2025. The second point is that CSIS shoulders the main burden of security screening for the Government of Canada. I'm going to come back to that point. Global Affairs has a subsidiary role in conducting security screening of locally engaged staff and other governments' officials at Canadian missions abroad. CSIS security screening is based on, effectively, assessing "loyalty to Canada, and reliability as it relates to that loyalty".

On the purpose of a CSIS security screening assessment, I'll quote from the Treasury Board directive:

> Assess, where sufficient information is available, whether there is reasonable cause to believe that the individual has engaged, is engaged or may engage in activities that constitute a "threat to the security of Canada," as defined in section 2 of the [CSIS] Act....

The final point is that CSIS is responsible for two separate streams of security screening advice. One is related to immigration files when red-flagged by IRCC and/or CBSA. The other is for Government of Canada security clearance approvals at different information access levels.

CSIS provides security screening advice according to the criteria I've mentioned. The advice is a judgment call based on the information available. As you've heard from Mr. Wernick, denial of a security clearance has serious ramifications for the applicant. Essentially, it means they are fired. Of course, denial can be tested through a complaint process adjudicated by the National Security and Intelligence Review Agency.

Judgment calls, which security screening advice is always a matter of, can be affected by incomplete information or inadequate management of data. In particular, looking into someone's future behaviour to decide whether they might pose an insider threat is always difficult, if not impossible.

The case that has prompted the committee's study may or may not be a spy case. I don't judge it in advance of the Belgian court process. An arrest has been made, and it is before the Belgian courts, as you know. That will no doubt complicate this study of the committee in terms of its access to some key documentation.

What I want to do is look past this case and offer the committee the suggestion that the current system for security screening in Canada is simply unsustainable. The dual burdens of immigration and security clearance screening on CSIS are simply too great. In my view, they threaten to erode the operational effectiveness of CSIS as it addresses its core missions. An intelligence service should not be a security screening shop.

Consider the statistics. In 2025, according to the "CSIS Public Report", CSIS received 129,130 requests under the government security screening program and 438,600 referrals for immigration and security screening. That is a total of 567,730—or 1,555 per day, assuming they arrive in an orderly fashion, which of course they don't. Buried in this mountain were 360 requests for what is called "foreign screening", defined as, "Security assessments to foreign governments, as well as to international organizations, when Canadians seek employment that requires access to sensitive information or sites in another country." Even with those relatively small numbers for foreign screening, the CSIS report indicates that there was a backlog in terms of their ability to deal with them.

An alternative model is already being practised by one of our closest allies, the United Kingdom. The U.K. has a separate, centralized organization for security clearances—in the U.K. system, it's called security "vetting"—that covers all government departments. U.K. security vetting was established in 2017, and since 2020 has been housed centrally within the cabinet office. It isn't left as a responsibility of MI5 or MI6 or any of the security agencies.

In my view, and this is my suggestion to this committee to give some consideration to, Canada should study and adopt the U.K. model, create a separate, centralized security clearance agency and divest one of its main intelligence organizations of this onerous responsibility.

● (1745)

Such a fundamental restructuring would also, in my view, create the circumstances for more coherent processes and better data management.

Should we, though, decide to stick with the existing model, there will be more recourse to AI usage, more outsourcing and continuing impossible burdens on CSIS. Which would you prefer?

Thank you.

[*Translation*]

The Chair: Thank you very much, Dr. Wark.

Mr. Haynes, you have five minutes.

[*English*]

J. Paul Haynes (Chief Executive Officer, Cinchy Inc.): Thank you, Mr. Chair.

Thank you, members of the committee.

My name is J. Paul Haynes. I'm with a company called Cinchy. We're doing security for AI. I've spent many years prior to that doing frontline cybersecurity with, probably, one of the largest organizations in the country that's in the private sector. I feel like a fish out of water here because I'm coming from that perspective, but hopefully that's useful to you.

I'm not going to focus on the specifics of the Belgian case, but I'm going to try to stick to the system and shape my remarks around things that we see that work in the private sector. There are a few key points, and some of this has been heard already.

The system is sound but it's static. The duration of clearances, five or 10 years without re-upping them, is completely at odds with how we would do things in the private sector. Anyone who's accessing financial records or securing them for banks, in the U.S. or anywhere else, is getting criminal and credit background checks every year. People change their behaviours if they have a credit problem. That's the number one reason we do that, just as an example.

The next point is the notion of “trust but verify”. I've dealt with this in private sector context scenarios where, if you're going to put extra monitoring on someone, you can't target them specifically. You have to trust but verify all of your team. That's a bit contrary to how, when we get a signal and we want to investigate the signal, from the human rights perspective our HR teams in the private sector are saying, “You can't target that person. You have to do that for everyone.” Trust and verify...it's easy to say but it has some challenges in practice.

The signalling that cybersecurity teams use to identify human behaviour, the synchronizing of the vetting and the way we do things on personnel versus cybersecurity, as I think we've heard in other comments, those things need to come together.

The information also exists but it's not connected, and there were a lot of examples that I was able to discover within the government. However, it occurred to us that having some sort of transferable integrity document, a passport for people who have clearances that gets maintained, might be a way that's going to get implemented—electronically, of course, that sort of thing—so that you would not have this disconnection of important data from the hiring managers in the new agencies that the new government groups are moving to.

Privacy also has to be balanced and not maximized. Through having an operation in Ireland, we saw scenarios in which the Irish had such extreme privacy protections that you couldn't compel employees to submit to credit and criminal background checks unless they were dealing with vulnerable people or children, or working for a police agency. That actually cut Ireland out of significant economic opportunities in aerospace and other security-related sectors. We have to get the balance right on this.

Then the other challenge, which has come up in different words, is having a limited verifiable history of new Canadians. Getting 10 years' history isn't possible for some of them, even though they might be the eligible candidate to work in the role. How do you trust another foreign government's agency, especially if they may have an interest in not necessarily giving the full story of the applicant or to help this country? We have some interesting challenges there. Again, you have to look at the risk level and put in mitigating controls that are commensurate with the risk level.

Where I would go in terms of recommendations—and I hinted at some of this—is to the notion of continuous evaluation, as the banks do. It works. It's not going to solve all of the problems, but it's not that expensive and it's very easy to do. There are a lot of private firms that do this. I'm sure the government has its own capabilities that could match it.

The notion of this shared integrity record that can bridge the PSC, the CBSA and the RCMP, among others that have a horse in the race, would probably go a long way to expediting this and ensuring that you have an integral view of that applicant in all their different roles. In the private sector this would happen, so I don't understand why we couldn't do it here.

As for connecting insider risk and IT security, we always talk about the worst-case scenario: How do you prevent a Snowden scenario? This is what we're talking about here. He was an insider, a contractor with Booz Allen, who had high privileges. When you see things like massive data downloads, which he was doing, they would be flagged. That sort of thing has to be connected, and then, obviously, there has to be additional oversight of external placements, as in this case we're talking about.

● (1750)

I can wrap up with this. Canada's system was built to check trust once and assume, and you know what happens if you assume. The greatest gains will come from connecting personnel security and cybersecurity.

I look forward to any questions.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you very much, Mr. Haynes.

Mr. Morrison, you have five minutes.

[*English*]

David Morrison (Senior Diplomatic and International Affairs Adviser to the Prime Minister, Privy Council Office): Mr. Chair and members of the committee, thank you for the opportunity to speak with you today.

As the senior diplomatic and international affairs adviser to the Prime Minister, I jointly lead the national security, intelligence and international affairs branch at the Privy Council Office. Within the Privy Council Office, my branch provides policy support to the Prime Minister, the Clerk, ministers and departments on matters relating to foreign affairs, defence policy, national security and intelligence, and we help coordinate across the government.

As I believe you are aware from previous testimony, our system here in Canada holds that individual departments are accountable for deciding to issue security clearances based on common requirements and informed by centralized expertise. The Treasury Board Secretariat establishes the policy framework. The public safety portfolio, through the RCMP and CSIS, contributes criminality checks and national security assessments, and individual departments collect relevant information, assess risks and make security clearance decisions under delegated authorities, with deputy heads remaining accountable for the integrity of those programs within their organization.

[*Translation*]

The allegations involving a Canadian citizen employed by the North Atlantic Treaty Organization have naturally raised questions about Canada's personnel security regime and the lessons that can be learned from this incident.

While Belgian authorities continue to lead the criminal investigation and Canada continues to co-operate fully with that process, the relevant departments have conducted reviews and made recommendations for potential improvements to the personnel security framework.

Having served as deputy minister of foreign affairs at the time the security clearance in question was granted, I note that Global Affairs Canada has informed the committee that its review found no breaches of the policies or procedures in effect at that time.

That said, this case highlights the importance of continually ensuring that decision-makers have the information, tools, governance mechanisms and safeguards needed to make the best possible security decisions in an ever-changing threat environment.

[*English*]

The Minister of Public Safety told this committee he has tasked departments with reviewing the case that has brought us all here and proposing process improvements. In a similar spirit, and in my Privy Council role of supporting the coordination of national security, intelligence and international affairs, I would offer some observations that I hope will inform the committee's consideration.

First, a government-wide repository or registry of security clearance information would improve efficiency, reduce duplication and help departments identify where relevant personnel security information may already exist.

Second, human resources-related information relevant to an assessment of an individual's reliability or loyalty should be available to personnel security decision-makers without compromising privacy protections or procedural fairness.

Third, open-source verification should be used more consistently across the government for a wider range of security levels. Its use would also benefit from common tools, training standards and methodologies across departments.

Fourth, a robust personnel security program should extend throughout employment through insider risk programs, continuous personnel security assurance, recurring screening, reporting obligations and security awareness, as the witness before me has just stated. These would help identify emerging risks, ensure that clearance-holders remain reliable and loyal, and ensure that clearances reflect current information.

Finally, I'm aware of suggestions made to this committee for CSIS, or even the Minister of Public Safety, to be the ultimate decision-maker in complex cases. I believe this would be a mistake. In our Westminster system, accountability for personnel decisions rests with the deputy head. That is by design and it has been codified in the Financial Administration Act.

● (1755)

I would add, for the record, that in almost six years as a deputy minister at Global Affairs and now going on four years in two different stints at the PCO, I'm not aware of a single case where security clearance was granted despite unaddressed concerns regarding a public servant's loyalty or trustworthiness.

Deputy ministers work collaboratively with the security services. In any complex case, I'm very confident that the clearance would either be denied or, in an extreme case, be approved with mitigation measures agreed upon with the security services.

I'm not able to comment on any individual cases today. I would be pleased to discuss the broader personnel security framework, governance considerations and ongoing efforts to strengthen Canada's personnel security system.

Thank you. I look forward to your questions.

[*Translation*]

The Chair: Thank you very much, Mr. Morrison.

We can now move to Ms. Kirkland for six minutes.

My apologies, it's actually Mr. Caputo's turn.

[*English*]

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

Thank you to the witnesses for appearing on this very important issue.

Through you, Mr. Chair, I will direct my questions to Mr. Morrison.

The Zhang case was and is a failure of our intelligence. Was it not?

David Morrison: I can't comment on any specific case.

Frank Caputo: Okay. Let's look at this just generally, and then we can get into hypotheticals.

I think you could comment, sir, on this: If we had somebody who went to a foreign nation on behalf of Canada because Canada had given them security clearance, and at the time the security clearance was obtained, they had a documented history of fraud in Canada, that would be a failure of intelligence—would it not?

David Morrison: I would say, in that hypothetical situation, all of the rules and protocols applicable at the time could have been applied. At the same time, systems can always be strengthened.

Hypothetically, information before a decision-making system could be acted on appropriately and decisions could be rendered appropriately and we could still get unintended outcomes. That's why I say there are systems that can be strengthened, and that's why I suggested four ways of doing so.

Frank Caputo: I'm mindful of that. What I'm saying is that when we have situations in which there is a documented history of fraud, that to me is the end of the discussion, because fraud is an integrity offence. It is an offence that speaks to your character. It isn't something you just do on a whim. I know you can't comment on the specific case, but Canada gave security clearance to somebody with a history of fraud.

I'll tell you this. We're very fortunate to have an intern in our office. She found the Zhang decision. As an intern of two weeks in our office, she was able to find the Federal Court decision. As she pointed out to me, people research people for a first date. They google this type of information and, I think, find it.

I will say it again. When the information is publicly available and we nonetheless give security clearance—high clearance, at that—that is a failure in intelligence. Would you care to comment?

● (1800)

David Morrison: My comment would echo that of my former colleague Tara Denham, who I believe testified here on October 7 and reviewed for members of the committee how GAC would be involved in such a case. I believe Ms. Denham also testified that even though it was not required at the time the clearance was given—therefore, all protocols were followed—GAC would now, for any similar fact pattern, indeed do an open-source search.

Frank Caputo: I would hope so. I think doing an open-source search is in itself a security failure. When I was a prosecutor, our security people did an open-source search for me, just to check on my safety, and this is somebody who is representing Canada.

At the end of the day, we gave security clearance, as Canada, to an alleged spy. It was not Canada, but Belgium that figured it out. We had a witness just earlier in the hour who said Canada is the most infiltrated country on earth. Fraud was known, and even after the decision was rendered on fraud, as backed up in a judicial review, Ms. Zhang continued with Employment and Social Development Canada despite the finding of fraud.

A French newspaper called it Canada's embarrassment. Does this not diminish our international standing with our Five Eyes allies and the G7?

David Morrison: For the record, I agree with the honourable member about the use of open-source, Google or however you want to characterize it. I think that should be a standard part of our vetting process.

I also agree, and tried to say so in my statement, that personnel information that speaks to someone's integrity should be part of the system. It was not part of the system at the time, and that has now been rectified, according to my colleagues at GAC—

Frank Caputo: We have only 40 seconds. I don't mean to interrupt you.

I misspoke when I said most infiltrated in the world. It should have been in the G7.

You were here at committee in 2023 because of foreign interference. You are very well aware of foreign interference. My colleague Michael Cooper questioned you about foreign interference around MP Chong and a report that was not forwarded. You said, “We have foreign interference. We have what the Indo-Pacific strategy calls—I might not get the wording right—an increasingly assertive China.”

This was on people's radars based on this, yet somebody got through at the highest level. How is that not a colossal failure of our intelligence?

The Chair: Answer very quickly.

David Morrison: I believe I've tried to answer that question. All of the relevant protocols and procedures were followed.

In the hypothetical case that I'm trying to respond to, if all protocols are followed and we have an unintended outcome, clearly the protocols need to be strengthened. That is the spirit with which I've come before your committee today, with suggestions for how to do so.

The Chair: Thank you, MP Caputo.

[*Translation*]

Mr. Ramsay for six minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): I'd like to thank all three witnesses.

If I may, I'll begin with a somewhat philosophical observation: I think we need to acknowledge that our system works quite well in over 99% of cases and that the cases we're examining today are rather rare. That said, I'm the first to want to improve the system. We have received a few suggestions from our witnesses today. Indeed, I believe the system needs to be improved, but we must be careful not to create a bureaucratic monster. We know that 500,000 audits are conducted each year in Canada, including nearly 130,000 for the public service and 400,000 for immigration.

Dr. Wark, you told us that, in your view, the British model—which separates the two entities—is the solution. With all due respect, I think that's a cosmetic fix to some extent. It's not about creating another agency. It could be that, but it's not that simple to create another agency that would, in effect, forgo the expertise of the Canadian Security Intelligence Service, which can contribute.

Mr. Haynes, you suggested certain measures to us. You did, however, tell us that there are nuances when it comes to confidentiality and privacy. You told us about the American model.

Essentially, my question to both Dr. Wark and Mr. Haynes is this: How do we create an effective system that improves upon what we're already doing, without creating a bureaucratic monster, with oversight that will require an incredible amount of resources? We must always remember that our system is quite effective and that it fails only in rare cases.

● (1805)

[*English*]

Dr. Wesley Wark: Briefly, I'll say I don't think anybody in the U.K. intelligence system believes they've created a bureaucratic monster by creating a specialized, centralized agency. I think they feel they've done the reverse.

The point I am trying to bring to you all is this: Do you really want an intelligence service that has a wide range of threats to consider, globally and domestically, bogged down bureaucratically and monstrously in the business of security screening, which isn't its main purpose?

We are very unique in this country in giving that security screening burden to one of our main intelligence collectors.

[*Translation*]

Jacques Ramsay: Dr. Wark, I just want to say that it's possible to have an intelligence agency with several units, where people have different roles. We don't ask the counterintelligence unit to conduct background checks. It is still possible to make certain distinctions within an agency.

[*English*]

Dr. Wesley Wark: It's all the same service—isn't it? That service, its director and its minister, who's accountable for it, have to make those kinds of resource allocations. How many people do we put in that area? How do we make sure that people in that area have other career opportunities? I could go on.

It makes no sense to me to have CSIS—and we are unique in the Five Eyes—continue with this job. We can continue with these practices and we can look to improve them, as some other witnesses have suggested, but I think we'll never get to the kind of system we're going to need. I fear that what will happen if we keep with the existing system, which would be a degradation of the service's capabilities in the key areas where we need them, is increasing reliance on artificial intelligence—you may or may not think that's a great idea—and, frankly, private sector outsourcing. Is that what you want?

J. Paul Haynes: I had some interesting experiences with our military. They have a cyber-force, and we had a number of first dates where we were trying to figure out how we could make our security operations team into reservists, so that they could be available in times of duress.

The fifth dimension of battle now is cyber. It's in all of the military discussions. They don't have adequate resources. They have adequate resources to deal with the day-to-day, but on a much broader scale, they don't. If we got into a time of duress or conflict, they would look to reservists, and we hit a wall on clearing: We could not get any efficient system. It's very expensive, as I'm sure everyone here knows, to get a secret level or higher, and we could not get past that.

Other countries have figured this out in different ways. Just from a national security perspective, if the private sector needs to become part of our defensive environment in a hurry, the system is very expensive. Maybe to Mr. Wark's point, it could be because you're using the sharpest instruments in the tool chest to do the work. A lot of it is very repetitive and mundane, so you could get some efficiencies there. AI has to be a part of the solution, without question.

We've talked about this from a government perspective so far today, but consider how you can extend into some of the initial industries, or industries we're trying to regenerate in aerospace, among others. These clearances are important when you're working with allied countries and training partners. Getting the private sector into the circle, where they're not now, increases our capacity from an economic perspective. These things get very integrated very quickly, and right now there are a lot of have-nots. All my colleagues in cybersecurity in Canada have had similar discussions. We have a hard time working with our own government.

● (1810)

[*Translation*]

The Chair: Thank you very much, Mr. Ramsay.

Mrs. DeBellefeuille for six minutes.

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

Mr. Morrison, I listened to you carefully, and I'm surprised. I agree with all of your recommendations because, ultimately, your goal is to improve the system. However, I wonder why these recommendations aren't already in place. That surprises me. How come they weren't in place before the Zhang incident? They seem quite justifiable, since the issue is well documented. Other witnesses have said that Canada is the G7 country most heavily infiltrated by China.

The improvements you're proposing make sense. However, why haven't these recommendations already been implemented? Given the positions you've held as deputy minister of foreign affairs and the role you currently hold as an adviser to the Privy Council, you're in a position to have all the information needed to recommend in advance that they implement the measures you're proposing here. That's what I'm wondering.

David Morrison: Thank you for that question.

I mentioned in my opening remarks that the Treasury Board Secretariat establishes the policy framework here. I'm almost certain that other witnesses appearing before this committee have already described the improvements that were implemented on January 6, 2025. That was the first time, I believe, since 2014—so in 11 years. I believe the circumstances that led this committee to conduct this study have shown us all that there is more work to be done.

Claude DeBellefeuille: I'm struggling to understand what you're telling me here. The way I see it, the Privy Council and its advisers are highly experienced individuals who advise the Prime Minister and his government. You can't possibly be telling me that the Zhang incident and our study led to these changes. I mean, that's giving us far too much credit. Thank you very much, but in my view, there were other spies before Ms. Zhang, and there were other incidents. I'm having a hard time believing that a major institution—a G7 country—is reacting to a single incident and a committee's study. I'll be honest with you—what you're telling me seems a bit far-fetched.

The other question I'd like to ask you—and I'm conscious of the time—is that another witness, Mr. Wernick from the Privy Council, told us that, ultimately, it's just a matter of political will: If the government considered it important to protect itself against espionage, it would provide its agencies and departments with sufficient resources to be able to cope with this challenge. He made that clear earlier.

Now, you're with the Privy Council. You can't reveal any secrets to me, but based on what we've heard, I expect that the next budget will include additional funding to protect us against interference and espionage, and that departments, agencies, and Crown corporations will be provided with the resources needed to carry out more effective screening. That's my understanding, because I'm a little taken aback by your last answer to my question.

● (1815)

David Morrison: I'd say that we're in the process of improving all our defence systems against foreign interference, espionage, and any threats. In a week or two, I hope, the government will launch a new national security policy. There's a major effort under way in this country right now to strengthen our defences against any threats. This will be the main focus of the new policy, which will be released shortly.

This is clear, at least to me and to many other witnesses, because I have reviewed the other testimonies. I believe this is the third meeting you've held on this topic. It's clear that, in the area of security clearances as well, more work needs to be done. I will do it, in my capacity at the Privy Council Office.

The Chair: Thank you, Mrs. DeBellefeuille.

[*English*]

It's MP Caputo first and then MP Lloyd.

Frank Caputo: Thank you, Mr. Chair.

I'll go back to Mr. Morrison.

I wanted to clarify something, sir. Am I correct in understanding your previous testimony to the committee as being that at the time Ms. Zhang received her security clearance, open-source checks were not part of the clearance process? Is that accurate?

David Morrison: My understanding is that at the time she received her clearance at the level she received her clearance, open-source checks were not part of the process.

Frank Caputo: Okay. Do you know what that clearance was? It would have been secret level, I guess, at least.

David Morrison: It was a secret level for NATO.

Frank Caputo: Right. You have basic, enhanced reliability, secret and top secret levels, and secret is up fairly high.

David Morrison: There are now six levels. There's—

Frank Caputo: The enhancements....

David Morrison: It's essentially like that, but each level has an enhancement.

Frank Caputo: Right. Do we know whether her level required the enhancement on secret?

David Morrison: I can't comment on any specific case.

Frank Caputo: Okay. For somebody at her level going to NATO, do you know?

David Morrison: I assume that somebody going to NATO requires a secret security clearance—yes.

Frank Caputo: Okay. Thank you.

Just so I'm clear as well, do you know whether now open sources are consulted on a secret-level clearance?

David Morrison: Yes, they are.

Frank Caputo: They are. Okay. You can't comment on this.

I'll call it my *obiter* that this is essentially a *mea culpa* when we start doing things differently after the fact.

With that, I'll pass it to Mr. Lloyd.

David Morrison: With respect, it's a tightening, a strengthening, of the system, which is the gist of what I tried to say in my opening statement.

Frank Caputo: I'm mindful of that. The timing is suggestive of the fact that it's a recognition that we weren't doing things to the best of our ability if we had to tighten that which was untight before.

Dane Lloyd: Indeed, yes.

Frank Caputo: Thank you.

Dane Lloyd: Thank you.

Mr. Wark, I want to talk about your proposal to go with the U.K.-style system. I always wonder when people come up with these proposals to set up a new secretariat or some sort of functionality.

Why can't we just give CSIS more resources to accomplish the same thing? What is the benefit of setting up a separate entity to carry out this process?

● (1820)

Dr. Wesley Wark: Thank you, sir.

It's a good question, and I guess the starting point for an answer to that question would be to look at the U.K. system, why exactly they moved in the direction they did and what they feel the strengths and weaknesses of that system might be. Learn from the U.K. experience. Keep in mind that Canada's approach to security screening is unique among the Five Eyes. Do we know something that our Five Eyes partners don't know about how to do security screening? I don't think so.

You can leave this function with CSIS. CSIS has had continual budget increases, fundamentally since 9/11. CSIS has, then, the job of proportioning how they're going to spend that money across the range of threats they have to deal with. Security screening will never be a top priority for them, nor should it be.

It becomes a very difficult calculation, then, for CSIS to say that we need this many people in the security screening portion of our agency and we're going to take people out of counter-intelligence, and we're going to take people away from the areas that are dealing with foreign interference and away from our overseas stations to do that. Is that what you want?

I just think that it makes much more sense—and it's not a question of creating some new bureaucratic monstrosity, as has been suggested—to take the existing expertise out of CSIS, put it into a centralized agency and be able to build the kinds of data systems and comprehensive processes that other witnesses have talked about. It's not that we add more bureaucracy. We add more efficiency, I would argue, through that process, but the starting point would be, “Let's learn from the U.K. model.”

Dane Lloyd: How much time do I have left?

The Chair: You have eight seconds.

Dane Lloyd: I appreciate that. I feel a bit like I'm in an episode of *Yes Minister* right now—

Voices: Oh, oh!

Dane Lloyd: —but thank you for that.

The Chair: Thank you for your indulgence, MP Lloyd.

Let me turn to MP Sodhi for five minutes, please.

Amandeep Sodhi: Thank you, Mr. Chair.

Thank you to our witnesses for being here today.

Dr. Wark, you mentioned that Canada is unique among the Five Eyes countries in terms of relying on CSIS to conduct security screenings, and you have also spoken about the U.K.'s approach. Are you able to elaborate on the approaches used by the U.S., Australia and New Zealand? Do they also have separate centralized bodies that manage the security screening process?

Dr. Wesley Wark: I'll be very brief.

My understanding is that all of our other Five Eyes partners have their own processes, and they all have different methods that they've developed for security screening and actual security classifications. The Australians and New Zealanders are fairly close in practice, as you might expect. My understanding is that none of those countries rely on their intelligence service to conduct security screening. Certainly, that is not the case in the U.S.

Amandeep Sodhi: Do you believe that the challenge that Canada is facing right now is primarily one of policy, resources, information sharing or organizational structure? How would you rank those issues?

Dr. Wesley Wark: That's a very large question.

What I would say, just for a moment for the committee, is that there's been considerable evolution in the approach to security screening and processes from 2014, when the first security screening standard, the new standard, was created—as Mr. Morrison referenced—down to an enhancement and some revisions in 2025. Much of that work has been conducted in reflection on concerns about insider threats. In the 2014 case, it was the impact of a major spy case, the case of the Jeffrey Delisle incident, where he offered his services to the Russian GRU. Therefore, we've been learning lessons along the way.

I think the policies are good policies. It is always impossible, I would say, to come up with a 100%-secure culture for dealing with insider threats. One of the things that many studies of insider threats point out is that very often insider threats develop after a person comes into a position of trust where they have access to sensitive information. You can have the best security screening practice, if you like, when you're giving a person access to a job and a classification, but it may not suit you down the road. Even there I would credit the government with the fact that it has been trying to deal with that problem.

I'll end on this point: It's no longer the case that we simply say to ourselves that we'll look at top secret clearance every five years and at secret clearance every 10 years. There has been a process under way since 2014 to engage in what's called aftercare—continuous monitoring of potential changes in people's behaviour or circumstances that may pose security risks, and a tightening of the periods of time within the five-year and 10-year periods where security clearances are being constantly reviewed. We've been trying to deal with that issue.

The policy is there. We have the right approach. I think it's just being done by the wrong agency, which is overwhelmed by the burden. There's no easy fix to that in terms of trying to shovel more money out the door to CSIS. I think it needs organizational change.

● (1825)

Amandeep Sodhi: Okay. Thank you for your answer.

I have just over a minute left. I will open up the floor to any and all witnesses.

If you have any further recommendations that you would like to get on the record, feel free to do so.

David Morrison: I would just say that, fundamentally, this is about risk management. In an increasingly tumultuous world, all risks have gone up. This will be detailed in the forthcoming national security strategy.

I appreciate Mr. Wark's comments that there has been a process of learning that has taken place between 2014 and 2025. I can assure you that if there has been a system failure that leads to an unintended consequence, we will further strengthen the system.

[*Translation*]

The Chair: Thank you very much.

Mrs. DeBellefeuille for two and a half minutes.

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

Earlier, my colleague Mr. Ramsay said we're talking about only one case and that it was an exception. I sensed a certain trivialization of the case we're currently examining, given the suggestion that it was almost an isolated incident. In fact, we have no way of knowing whether there are many cases, since perhaps some spies haven't been caught yet.

This is what we're interested in, and I understand it's very important. Mr. Morrison, you said that the fact that the Zhang case was publicized and is being examined by the committee served as a sort of wake-up call for the government. You also said that everyone had gotten to work and started proposing solutions to improve the system, because there are more and more attacks, interference and infiltration by foreign countries in Canada. That served as a wake-up call for us. That's what I sensed when you answered me earlier. If the system had been working, you wouldn't have said that you're proposing a series of actions to be taken. You even gave us an exclusive—at least for me—by saying that we're going to launch a national policy on national security very soon, given how urgently we need to respond to the current level of risk affecting us.

Am I understanding this correctly? Were you truly shocked when you learned what had happened in the Zhang case?

David Morrison: Once again, I cannot discuss a specific case.

I would say that what might happen in Canada has already happened in several other countries. Recently, as Dr. Wark knows full well, there was a shocking incident in Germany. It was a disaster, and it involved someone from within the system.

In my remarks, I mentioned a few ideas for strengthening our system. However, as I just said, ultimately, it's a matter of risk management.

● (1830)

[*English*]

We're not living in a world with zero risk. Systems can always be strengthened. The government and the bureaucracy are committed to continuous improvement in all our national security systems.

[*Translation*]

The Chair: Thank you very much.

Ms. Kirkland—

Claude DeBellefeuille: Excuse me, Mr. Chair, I would like to thank Mr. Morrison for making a great effort to speak in French throughout his testimony and when answering my questions.

Mr. Morrison, I'm touched because senior officials at your level often lose their French since they work so much in English. I wanted to tell you that. I'm truly grateful for your efforts. Thank you very much.

David Morrison: I'm an ordinary guy from Lethbridge, Alberta.

The Chair: We recognized the Lethbridge accent.

David Morrison: It wasn't easy.

The Chair: It was excellent.

Thank you, Mrs. DeBellefeuille, for your very generous and relevant comments.

Ms. Kirkland for five minutes.

[*English*]

Rhonda Kirkland: Thank you, Mr. Chair.

I'm pretty fascinated by the "tightening of our system" comment that was made regarding open source and looking at open source. It feels like the most common-sense thing to do, the first thing to do, would be, "Let's google these people."

You mentioned earlier, Mr. Morrison, that clearance will be denied if someone is found to be untrustworthy. You would agree, I'm sure, that fraud would be an example of a trustworthiness test that has failed.

David Morrison: I would agree in a hypothetical case.

Rhonda Kirkland: Hypothetically...yes.

David Morrison: In a hypothetical case, if full awareness of a candidate included awareness of documented fraud, that would speak to that person's trustworthiness.

Rhonda Kirkland: You would say, then, that if there was a hiring process for NATO and Global Affairs saw anything to do with fraud from an individual, that individual would likely not receive their security clearance. That's if they were aware of it.

David Morrison: If Global Affairs had been aware of anyone who had derogatory information that would speak to that person's suitability and reliability to protect Canada's secrets or NATO's secrets, I have every confidence they would have acted on that information.

Rhonda Kirkland: Thank you. I appreciate that.

We've established that open-source checks at one time were not part of the hiring process for security clearances, which, again, I will say I find quite shocking. You believe that the system has been tightened and that now we do. To me, if you have to tighten a system, that means there was a breakdown. There was a failure in that system; therefore, we had to tighten it and make sure that didn't happen again.

Help me understand this. I'm going to try to explain it as best I can. If someone needs a security clearance and we know the open-source process was not part of it, would we not have a search for any federal or provincial court records for that or any person?

David Morrison: There are a number of elements, as I think colleagues have testified before this committee, that go into a security clearance evaluation.

Rhonda Kirkland: Yes, absolutely. I'm just—

David Morrison: One of them comes from CSIS and looks at national security, and one of them comes from the RCMP and looks at law-abidingness. There are also credit checks. Those are the procedures that would be in place for someone applying to NATO. My colleagues from Global Affairs have assured me that they have added to that protocol that an open-source search also be conducted.

Rhonda Kirkland: Good. I'm glad to hear open source has been added, but it sounds like a Federal Court database or provincial court databases would be searched to see if there were any instances of a person having been part of Federal Court.

In July 2023, just to put it out there, Zhang initiated a judicial review, which was part of the Federal Court document of August 22, 2024. She received a position at NATO at the beginning of 2025, so it was pretty recent. A simple search of whether there were Federal Court documents with that name in them should have flagged it.

If what you're saying is true—that in a general sense, we would be looking for court documents on a person if we were giving them a security clearance—that is an example, clearly and purely, of a system failure.

● (1835)

David Morrison: I don't think I said that in a general sense we would be looking for court documents. What I tried to describe was the role of CSIS, the role of the RCMP and the role of GAC in granting a security clearance for someone going to NATO. I've also said, I think quite clearly, that according to the protocols in place at that time, GAC did not require an open-source search. They now do.

Rhonda Kirkland: I understand the open-source portion. My concern was a search for Federal Court documents and whether that would be part of a security clearance check.

David Morrison: The law-abidingness, if I can put it that way of a person is meant to be looked at by the RCMP.

Rhonda Kirkland: The RCMP could have made a check—

The Chair: I'm very sorry to interrupt, MP Kirkland. That was a good intervention.

MP Powlowski, you have five minutes, please.

Marcus Powlowski: Mr. Wark, I would assume that you know how committees work. You were very succinct in making a recommendation. You said the current system of security screening is unsustainable. CSIS, as it is, has to clear 480,000 immigrants per year plus these security screenings, so there are 520,000 cases a year.

The U.K. has set up a separate security screening system. Is that for all government employees? Is that all the U.K. body does?

Dr. Wesley Wark: Thank you for the question, sir.

The U.K. security vetting office, as it is called, grants security clearances across all government departments and agencies in the U.K. It's a centralized unit working out of the Cabinet Office that covers the breadth of the U.K. government.

Marcus Powlowski: You're suggesting we make some sort of recommendation, like the Government of Canada should consider creating an independent security screening agency for government employees. Is that what you're suggesting?

Dr. Wesley Wark: That's a brilliant idea, sir.

Marcus Powlowski: We have here a member of our government and someone who is quite high up.

Mr. Morrison, in a way, I hate to put you on the spot, but I'm assuming given your position, you've been put on the spot before.

What do you think of this idea?

David Morrison: I've given you four examples of areas that my colleagues at the Privy Council Office and I think could usefully be implemented to strengthen the current systems. I would ask you to pay attention to number four in particular, which is the continuous evaluation. The first three are about the initial screen. The last one, about continuous monitoring, insider risk programs and so on, is the key, and emphasis should be put within that on self reporting. If somebody's financial circumstances change, if somebody gets married to somebody new or if somebody gets married in general, that is information that people need to disclose, because it could change their risk profile.

To be quite honest, I've not given any thought to where the capacity should sit. I just finished explaining that it is not solely a CSIS thing. It's not solely an RCMP thing. It's not solely a GAC thing. If I were where you are, I'd ask Mr. Wark this question: Isn't CSIS going to end up doing a lot of the work anyhow because a centralized agency may have to rely upon CSIS systems?

Quite frankly, I think culture and protocol around security awareness is much more important than structure. The function can be centralized at CSIS and firewalled off. I work at the Privy Council Office. I've never been one to create a greater PCO. I think the ballast of work should be done in line departments, but that's what people from PCO always say.

● (1840)

Marcus Powlowski: Quickly, I'd like to ask Mr. Wark to respond to Mr. Morrison's suggestion that CSIS is going to end up doing all the work anyhow.

Dr. Wesley Wark: I don't think that would be the idea. That would be an outcome you wouldn't want. What you would want, of course, as Mr. Morrison has indicated, is a central agency with access to CSIS material. You would want a central agency with access to RCMP criminal databases, the Canadian Police Information Centre and so on. You would have one agency that could draw on those resources without CSIS having to deploy its own people to do that work.

The Chair: Thank you, MP Powlowski.

[*Translation*]

I'd like to thank our three witnesses—Dr. Wark, Mr. Haynes, and Mr. Morrison—for participating in and preparing for this important meeting. I hope they enjoy the rest of their day. We will now let them quietly leave the meeting.

[*English*]

We are almost at the end of the meeting, but I believe that MP Caputo wanted to table a notice of motion.

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

As people have seen, parole has been at the centre of a number of questions I've asked in the House of Commons of late. I recently met with the mother of murdered 10-year-old Heather Aspin-Thomas and her counsel, Rebecca Darnell. I've done a fair amount of work as well on other files relating to parole. Brock Graham is a recently released federal offender. I've done some work on that matter.

After speaking with the victims, I believe the motion I hereby give notice of is appropriate:

> That, pursuant to Standing Order 108(2), the committee undertake a study examining the policies, practices and procedures of the Parole Board of Canada and their impact on victims of violent crime and their families.
>
> That the committee dedicate no fewer than five meetings to this study; that the committee invite the Minister of Public Safety, the Chairperson of the Parole Board of Canada, the Federal Ombudsperson for Victims of Crime, and any other witnesses the committee deems appropriate; and that the committee report its findings and recommendations to the House.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you very much, Mr. Caputo. It will be translated in both official languages.

Members of the committee, I'd like to inform you that, next Monday, we will be hearing from witnesses as part of our review of Bill C-236 introduced by Mr. Lloyd. The following Wednesday, we will conduct clause-by-clause consideration. That said, amendments must be submitted by Friday, October 23. There will be other business the following week, but we will set aside time to discuss it.

Thank you very much for your attention and participation.

Have a good evening.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: https://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : https://www.noscommunes.ca