



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

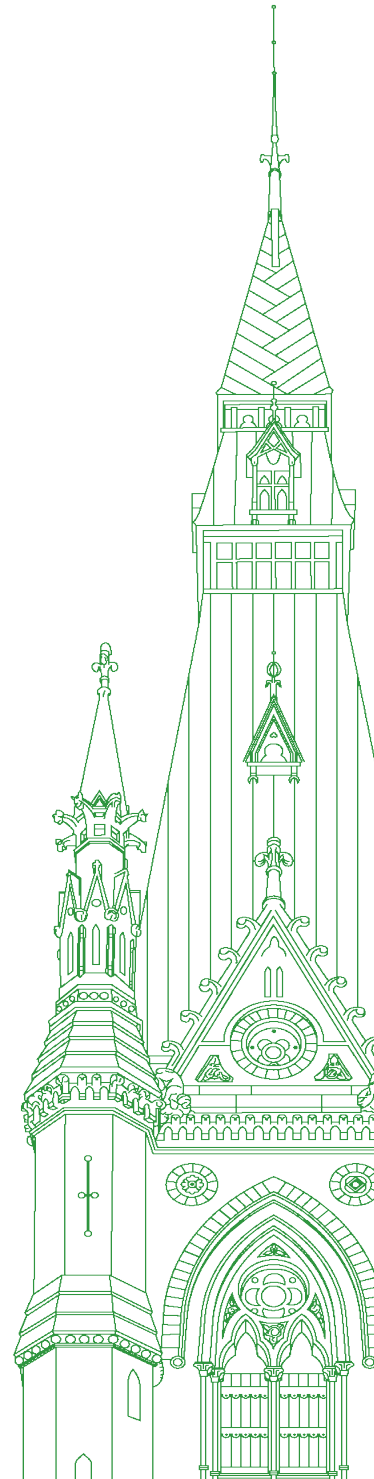
Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 050

Wednesday, October 7, 2026

Chair: Jean-Yves Duclos



Standing Committee on Public Safety and National Security

Wednesday, October 7, 2026

• (1635)

[Translation]

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

Good afternoon, everyone. Welcome to meeting number 50 of the House of Commons Standing Committee on Public Safety and National Security.

Before we begin hearing from the witnesses, I would ask the committee to consider, and potentially approve, the two requests for project budget that the clerk distributed to members yesterday. The first budget relates to Bill C-236, an act to amend the Criminal Code, the Corrections and Conditional Release Act and the Prisons and Reformatory Act. The second budget relates to the study we are currently conducting on Canada's security screening process. As you know, these are estimates. The committee may spend less. If so, the remaining balance will, of course, be returned to the Liaison Committee.

Are there any questions for the clerk or for me? May I take it that the budgets are adopted?

Some hon. members: Agreed.

The Chair: The two budgets having been adopted, we can now proceed to the main business before us today.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Monday, August 17, we are meeting as part of our study of Canada's security screening process.

I'm pleased to welcome our witnesses from two organizations. From the National Security and Intelligence Review Agency, we have Craig Forcese, vice-chair; Nathaniel Fournier, director-general, review; and Lawrence Mangano, acting executive director. From the Offices of the Information and Privacy Commissioners of Canada, we have Philippe Dufresne, Privacy Commissioner of Canada, and Marc Chénier, deputy commissioner and senior general counsel.

Each organization will have five minutes for opening remarks. We will begin with Mr. Forcese and conclude with Mr. Dufresne.

Mr. Forcese, you have the floor.

Craig Forcese (Vice-Chair, National Security and Intelligence Review Agency): Thank you, Mr. Chair and members of the committee.

[English]

Good afternoon. Thank you for your invitation to appear today.

As noted, I am the vice-chair of the National Security and Intelligence Review Agency, or NSIRA, and I am joined by our secretariat acting executive director, Lawrence Mangano, and the director general of review, Nathaniel Fournier.

Today I will address three points. First, the process used in security screening has sometimes been uneven across files. Second, the processes are often very slow, and third, the methods used sometimes raise concerns about their suitability.

Before getting to my points, let me make a few contextual comments.

[Translation]

First, NSIRA has two core responsibilities. The first is to review national security and intelligence activities to assess whether they are lawful, reasonable and necessary. The second is to investigate public complaints related to national security and intelligence, including those involving denied security clearances. In doing so, we provide independent assurance to Canadians that these activities comply with the law as it exists.

Second, regarding the incident in Belgium, NSIRA does not have fact-specific knowledge about this case and is unable to comment on the matter. Rather, my purpose this afternoon is to share unclassified observations on the security screening process stemming from our existing reviews and complaints investigations.

[English]

On this matter, security screening is the primary mechanism for determining whether individuals can be trusted with access to sensitive information facilities and national security activities.

Security screening also balances different objectives. If someone is denied a security clearance, the department mitigates security risk. However, this denial could entail the loss of a public sector career. The security screening process is therefore designed to be effective, rigorous, consistent and fair.

I turn to my three specific points.

[Translation]

First, in our public complaints investigations, we have found many security clearance processes met proper standards. However, some security screening reports to departmental deputy heads omitted information that supported the screened individual or inaccurately summarized their interview, creating a sometimes uneven process across files.

[English]

Second, screening can take a long time, leaving prospective employees in a prolonged state of uncertainty and departments without the personnel they require. In a special report that will soon be tabled in Parliament, we address the systemic delays in immigration security screening, which shares some similarities with the government security screening process.

Third, the methods used for security screening have also sometimes raised concerns about their suitability.

[Translation]

In particular, NSIRA and its predecessors have conducted several reviews of the use of polygraphs for enhanced top secret clearances by the Canadian Security Intelligence Service, or CSIS, and Communications Security Establishment Canada, or CSE. Our predecessor raised concerns about CSIS's use of the polygraph and the polygraph's accuracy more than seven times.

• (1640)

In our own 2019 and 2023 reviews, we concluded both CSIS and CSE placed determinative importance on polygraph examinations, despite their questionable accuracy and reliability in detecting dishonesty. We noted several practices raising concerns about the legality, reasonableness and necessity of polygraph use.

[English]

To conclude, safeguarding government information depends on a security screening process that is effective, rigorous, consistent and fair. Scrutinizing the government's ongoing security screening practices remains, therefore, an ongoing preoccupation for NSIRA.

[Translation]

Thank you. We would be pleased to answer your questions.

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

I now invite Mr. Dufresne to take the floor.

Philippe Dufresne (Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada): Good afternoon, Mr. Chair and members of the committee. Thank you for inviting me today to speak to the committee's study of Canada's security screening processes. With today is Marc Chénier, deputy commissioner and senior general counsel at the Office of the Privacy Commissioner of Canada.

Having a valid security clearance is a condition of employment in the Government of Canada. It is also required in other cases, such as the awarding of government contracts. Individuals provide consent for the collection, use and disclosure of their personal information for this purpose and the nature and extent of that collection will vary depending on the level of security clearance required.

[English]

My office, the Office of the Privacy Commissioner of Canada, is involved in the security screening program from two perspectives, first as an employer, in applying requirements to our own employees to ensure that they possess the requisite security clearance, and then as a regulator, in overseeing federal institutions' processes as they relate to their employees' personal information, including by investigating complaints received and providing advice to the Government of Canada on its policy requirements and their implementation.

In furtherance of individuals' privacy rights with respect to the federal government, the Privacy Act imposes restrictions and obligations on federal institutions' collection, use and disclosure of personal information, and it protects the personal information that they hold. While the Privacy Act outlines certain requirements for institutions, it does not present any overarching barriers to the collection or disclosure of personal information associated with security screening. Section 4 of the act allows for the collection of personal information that directly relates to an operating program or activity of a government institution, which may include security screening activities.

Over the years, the OPC has provided input to the Treasury Board Secretariat on policy instruments, including the federal directive on security screening, which establishes the high-level parameters governing how federal institutions screen employees who hold or are seeking to obtain a security clearance. My office has highlighted the importance of evaluating the necessity, proportionality, effectiveness and minimal intrusiveness of collecting personal information for the purpose of security screening.

We have also underlined that this evaluation will be particularly important in the context of open-source inquiries, polygraph testing and security clearance maintenance to ensure that the means will yield accurate information, and therefore be effective, and that there is no less privacy-invasive means to achieve the same ends.

[Translation]

In order to ensure consistent protection of personal information, my office has encouraged the Treasury Board Secretariat to provide federal institutions with meaningful and detailed guidance around the directive, including on how organizations should assess and mitigate the risks associated with this screening.

The act also allows me to initiate an investigation if I am satisfied that there are reasonable grounds to do so.

[English]

In January of last year, I commenced a review of polygraph use by government institutions. The investigation is ongoing, and I look forward to sharing my findings upon completion of this investigation.

Thank you again, and I look forward to your questions.

[Translation]

The Chair: Thank you, Mr. Dufresne.

We will now proceed to the question period with members.

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

[English]

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

Thanks to the witnesses for their time today.

By way of review, on Monday, this committee heard directly from the Minister of Public Safety and senior government officials about Canada's security screening system. The minister acknowledged that there are gaps in the system. We also heard that CSIS and the RCMP have provided recommendations for reform.

We know the study began because, previously, a Canadian was found to have committed fraud in a federal hiring process after applying to the Canada Border Services Agency under different names, yet she was still able to obtain a security clearance for an internship at NATO headquarters. She is now facing serious espionage allegations in Belgium.

For me, what makes this case particularly troubling is how widely this individual was able to move throughout the federal public service. According to the limited information available, Ms. Zhang was employed by the Canadian Space Agency, Statistics Canada, the National Research Council, and Employment and Social Development Canada before ultimately obtaining the NATO internship. This should be deeply concerning to every Canadian. In my opinion, it's an extraordinary failure of confidence in Canada's security screening system. Frankly, it's embarrassing for Canada on the international stage. I think our allies expect Canada to protect sensitive information and to know whom we are giving access to.

Mr. Forcese, my first questions are for you.

The minister acknowledged on Monday that there are gaps in Canada's security screening system. From NSIRA's review work, what are the most significant vulnerabilities you have identified in the federal security screening?

• (1645)

Craig Forcese: Thank you for the question.

In terms of our data bank, about which I can answer, our reviews have focused on a subset of departments. CSE and CSIS have been the subject of our reviews on internal security matters.

In our complaints work, we've looked at several different departments. Individuals who are discontent with a security clearance outcome can bring a complaint. The investigation that implicates... The deputy head of that individual department has the authority to

issue, or not, a security clearance. This means we have partial insight, not comprehensive, across-the-forest insight, as to the circumstances that the system now confronts.

I will say, based on our review work, that there are disparities, as there are many different decision-makers who will ultimately determine clearance decisions within departments. There can be disparities in terms of the application of what is supposed to be a comprehensive and singular process issued by Treasury Board. I mentioned some of the inconsistencies we've observed in our complaints work.

In terms of the question you raised earlier about the prospect of siloed information—I think that was the premise of your question—it's not something we've been able to track, in the sense that we haven't done a cross-departmental review. However, in our other review work, siloed information in the community writ large is an extant issue that we see and discuss regularly. Therefore, if there are silos, it's not something we've not encountered before.

Rhonda Kirkland: Thank you.

This is a primary concern. If someone applies for a job in the public service, there are founded allegations of fraud, and then they apply for another position, it feels as though those who are hiring—who are in that position in the public service—should know this happened somewhere else.

I'd like to move on to Mr. Dufresne, if I may.

You mentioned to us that the Privacy Act does not present any overarching barriers to the collection and disclosure of personal information associated with security screening.

Is it fair to say that the privacy law itself should not prevent relevant information about an individual from being shared for security screening processes? For instance, could one public service hiring manager—for lack of better words—find out if they've tried to apply somewhere else in the public service and were denied because of fraud, and does this infringe in any way on their privacy rights?

Philippe Dufresne: As a general principle, privacy is not an obstacle to national security. It is not a zero-sum game. We have the concepts of necessity and proportionality—looking at what is needed to perform the function. When we're dealing with cases, whether it's collection or use.... Was it necessary? Were we using too much? Were we collecting too much, and was it proportional to the threat?

In the context of security assessments, you're going to look at the nature of the job and the nature of the risks, making sure you have enough information to make your assessment in the best way possible. It's about not getting too much information or information that is irrelevant. It's about getting what you need for your task.

• (1650)

Rhonda Kirkland: Apparently, the deputy heads make the security clearance decisions, according to what the public safety minister said.

Can information be made available to them about someone applying who's tried to apply somewhere else and committed fraud in that application?

Philippe Dufresne: We'd have to review the specific details of what's going on. I haven't investigated this particular case or situation.

In terms of sharing information, our advice is to look at the necessity of it and at the legal authority in your mandate, making sure that you have agreements for how you're going to care for this information and that you have transparency and awareness. When we're dealing with the breach of Canadians' information or when governments hold personal information, we encourage departments to work with one another to keep one another informed. If there are gaps....

Treasury Board is recommending a review of the Privacy Act to allow greater sharing of information among departments. That would be up to Parliament.

[Translation]

The Chair: Thank you, Mr. Dufresne.

Ms. Dandurand, you have the floor for six minutes.

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

I'd like to thank all the witnesses for joining us for this very important study.

I will start with the representatives of the National Security and Intelligence Review Agency.

From your perspective, if we had the best possible security screening system, what would it look like? What types of information would be collected? How centralized or decentralized would it be?

Craig Forcese: I will start with some observations concerning our role.

[English]

Our task is to retrospectively review the conduct of the Government of Canada. In context, we have findings and make recommendations to improve the system.

Generally speaking, we're reluctant to speculate outside the context of having conducted this sort of assessment for fear that, having proposed certain changes—if, subsequently, we review—we'll be accused of marking our own homework.

You asked me what we might envisage as ideal. We cannot articulate a vision right now. We would have to react to the system that exists, probe its shortcomings or virtues, and then make observations accordingly.

[Translation]

Marianne Dandurand: All right.

It has nonetheless been proposed that the screening process eventually become more centralized. In your view, would greater centralization reduce its effectiveness?

Craig Forcese: I believe you're referring to a single decision-making authority.

[English]

Based on our experience, as I mentioned before, there have been inconsistencies that we've observed in the approach taken by different departments in relation to what otherwise is supposed to be a single standard, one first articulated—in terms of our review—in the 2014 security screening standard and now in its latest iteration, from 2025.

To the extent that you have a multitude of different decision-makers running their bespoke processes in alignment with the comprehensive rules, you would expect some variability. A centralized system might avoid that.

[Translation]

Marianne Dandurand: Is it possible that security clearance requirements differ from one department to another, or should they be the same regardless of the department involved?

[English]

Craig Forcese: In terms of the standards themselves, different departments—even different individuals within departments—might have different needs with respect to level of access and information. This is why you have the gradation and different security clearance standards.

One would assume that a similar standard should be assessed according to a similar set of protocols and against a similar set of criteria.

[Translation]

Marianne Dandurand: Thank you very much.

Mr. Dufresne, when an individual is hired by the government, they must consent to security checks. Does that consent extend to open-source checks, such as reviews of social media? Should the consent forms specify that explicitly?

• (1655)

Philippe Dufresne: That will depend on the nature of the security clearance being assessed. Open-source checks are possible. We've made recommendations to departments in that regard to ensure transparency and to avoid simply assuming that, because information is available from an open source, there are necessarily no privacy protections that apply. The appropriate approach is still to obtain only what's necessary and nothing that goes beyond that. The process must also be transparent. People should be aware of what's involved when they take part in it. They should be informed about what's expected of them because this is a condition of employment. The necessity and proportionality of the screening will depend on the level of clearance required.

Marianne Dandurand: If departments conduct these checks, what do the rules look like with respect to retaining information and correcting information that's inaccurate?

Philippe Dufresne: Departments have obligations regarding the retention of information under the Privacy Act. They must keep that information for a prescribed period.

There are also requirements to safeguard information in order to prevent leaks and privacy breaches, although those requirements are not yet set out in legislation. They exist under Treasury Board policies.

One recommendation I have made, and I'm pleased to see it reflected in Treasury Board's current consultation on modernizing the act, is that departments should have a legal obligation to implement proportionate measures to protect information. One can readily imagine that this information may be extremely sensitive in nature. The higher the security level, the more sensitive it becomes. We see that, for example, in the context of polygraph examinations.

Marianne Dandurand: I have 30 seconds left. I will use the time to thank you again for being here with us. I don't believe I can ask a new question in 30 seconds. Thank you very much.

The Chair: Thank you, Ms. Dandurand, for your customary graciousness.

Mrs. DeBellefeuille, you have six minutes.

Claude DeBellefeuille (Vallée-du-Haut-Saint-Laurent, BQ): Mr. Forcese, I may have misunderstood, so I'd like to verify something with you.

On seven occasions, you informed the government that there was a problem with the polygraph, either because of overreliance on it or due to its lack of reliability. You raised the issue seven times, yet it doesn't seem to have had any impact or influence, since the Canadian Security Intelligence Service and other agencies continue to use the polygraph as an indicator in assessing security. Have I understood correctly?

Craig Forcese: The situation is actually worse than that: Our predecessor raised concerns seven times, and we've done so twice ourselves, so that brings the total up to nine times.

Claude DeBellefeuille: So it's nine times. I don't know whether you're aware of this, but I greatly appreciate the work of the National Security and Intelligence Review Agency, and I believe it's my responsibility to highlight that work, because I don't understand

how a government can set aside nine recommendations from an agency whose primary mandate is oversight and investigation.

Let me ask another question. The minister came before us and stated that, with respect to the case of the alleged NATO spy, he had directed his department to investigate quickly. Was that investigative mandate assigned to your agency, given that this is your specialty? Did you receive a mandate from the minister to conduct such an investigation?

Craig Forcese: No.

Claude DeBellefeuille: Would you have been able to conduct a quick investigation in Ms. Zhang's case? Do you have the resources and expertise to conduct such an investigation?

[English]

Craig Forcese: In terms of our review work, a number of considerations would drive our priorities in the review space, including the attention a matter is generating in the interest of parliamentarians. In deciding how to scope a review, we would be preoccupied with making sure that our observations were sufficiently systemic.

Our task is to review the conduct of the Government of Canada, not the conduct of private individuals. Our focus would always be on looking at the government activities, not trying to conduct a collateral investigation of an individual.

• (1700)

[Translation]

Claude DeBellefeuille: So, basically, what I understand is that if the minister had asked your office to investigate, to make it a priority and to instruct his department to provide you with all the necessary information within a set time frame, you could, as a monitoring and investigation specialist, have investigated the case presented to us today for consideration, namely Ms. Zhang's case.

[English]

Craig Forcese: We would have the competence to see all information in the possession or control of any of Canada's national security agencies, with the exception of cabinet confidences. We would ingest that information, run it through our internal methodology to ensure quality control, conduct the factual accuracy exercises we engage in and issue a report. Our reports would then go to the minister. In some circumstances, redacted versions of our reports would, after the redaction process, become public.

[Translation]

Claude DeBellefeuille: All right.

What I see, then, is that the minister deprived himself of your expertise and experience in the case we have before us today.

I know you have carried out other studies in the past. Take the case of Jeffrey Delisle, which you investigated and found to have involved shortcomings and a lack of rigour in the process, including in the review of his security clearance. Security clearances at the secret and top secret levels are reviewed in accordance with the terms set out in Treasury Board policy and, in the case of Jeffrey Delisle, the naval officer, you determined in your investigation that the reassessment had not been carried out correctly.

So I have a lot of questions: If the minister thought the matter was so important, why didn't he give you a mandate to investigate Ms. Zhang?

I look at your public reports and I know, for example, that an investigation begun in 2023 was completed in 2026. So, naturally, I find myself thinking that the minister perhaps considers you too slow in reporting on your investigations, but I think I understand why. At present, I know that you have produced a report on national defence that you wish to make public, but that this department is taking legal action against you, prohibiting you from publishing it, and that the Canadian Department of Justice is supporting this department in preventing you from publishing your report.

I question how seriously the government takes your agency. We have proof: You wish to publish a transparent report on defence, but the government is opposing this through two bodies, two departments. Furthermore, it is not seeking your assistance at all in Ms. Zhang's case.

So I think one of the recommendations we're going to make is that the agency be considered in cases like this as an independent, very important agency to consult from the outset, rather than requesting an internal review of its own departments.

The Chair: Thank you, Mrs. DeBellefeuille.

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

[English]

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

I'd like to thank all of our witnesses for being here.

One of the things that struck me from the minister's testimony last week and got me thinking is that we often talk about how not everything can be known. I think an ex-CSIS director said that. There will be things that aren't always known.

The problem is that some mistakes in life are bigger than others. A nuclear meltdown is a one-time mistake, for instance. I know it's an extreme example. The point is that, sometimes, you aren't really in an arena in which mistakes can be made, because, eventually, the repercussions are so severe. We don't really get a mulligan.

It's against this backdrop that I was thinking about this. What is so troubling about the Zhang case, in my view.... I know you may not be able to comment specifically on the case, but you can certainly comment on the circumstance. The circumstance is this: Everything was knowable. Everything was there to be seen. She had lied on an application. The red flags were present. This isn't just a matter of not getting the right references or calling the right people. This was a matter of—I'll be blunt—failure at some level.

Can somebody comment on that, please?

Philippe Dufresne: We have not investigated this specific situation, but when we look at privacy breaches that happened in government departments, we look at them in this sense: What happened? Could it have been prevented? Were the mechanisms in place sufficiently robust? Were they followed appropriately? Were the standards the right ones? Was there enough communication among the senior decision-makers? Was it quick enough? Was there

enough reaction time? We look at whether it should have happened and what lessons can be learned to correct it. We look at things like robust safeguarding, siloed information and risk.

Certainly, necessity and proportionality would say that the greater the risk, the greater the safeguards.

• (1705)

Frank Caputo: Go ahead, please, Mr. Forcese.

Craig Forcese: We would do much the same on our complaint side. We would look at the information collected in support of a security clearance process, and we would ask whether the information was accurately conveyed to the ultimate decision-maker. Now, those processes are driven by persons who are discontented with the outcome, so we're ensuring that procedural fairness and substantive fairness have been observed.

I will say that in our review work—in which we look more systematically, at least, at the practices of individual departments such as the CSE—one of the observations we've made for both the CSE and CSIS is the primacy they put on a polygraph. In our recent 2023 focus on the CSE, this primacy meant that other facets that might reasonably be employed for purposes of conducting a thorough security clearance were not being pursued to the extent that we believe would be warranted. When you talk about the prospect that steps might be missed, this is the sort of observation we have made in the past.

Frank Caputo: I'd like to build on that, please, Mr. Forcese, and this is why.

In the case of a polygraph—and I'm far from a polygraph expert—you have an examiner who subjectively interprets the results. Now, that person is highly trained—don't get me wrong—but you have false positives and maybe some false negatives. False positives are the ones people often really care about, but false negatives can be just as bad. That's somebody who's interpreting the results. It's like, “Okay, did we get it right or not?”

In the Zhang case, there was objective evidence in that there was a finding of fraud. In fact, there was a finding of fraud in a case that was a reported decision—I believe it was a reported decision, but I'd have to double-check that. For example, it's on a website, that type of thing. When we talk about polygraphs, I guess I'm not sure if I would go down that path. This was so blatantly available. Is this not just a failure?

I'm mindful of your limitations. I'm not trying to put you in a box. However, when there's concrete evidence... It's not “Do we think this or not?” This person committed fraud while an employee of the federal government. Is it not a catastrophic failure if we don't know that somebody committed fraud or if—the alternative—we give them a security clearance, knowing they are fraudulent in the information they provide?

The Chair: Unfortunately, that was a great question—

Voices: Oh, oh!

The Chair: —but there is no time for a great answer. I need to turn to MP Housefather for five minutes, please.

Anthony Housefather (Mount Royal, Lib.): The theatrical flourish at the end of Mr. Caputo's questions was so amazing.

I'm going to ask Mr. Forcese a couple of questions.

Mr. Forcese, I heard your answer to Madame DeBellefeuille that at this point the agency has not unilaterally decided to review the activity carried out in the Zhang case. Did you make this decision because your interpretation of paragraphs 8(1)(b) and 8(1)(c) of the act is that you can only review an "activity carried out by a department that relates to national security or intelligence" and a "matter that relates to national security or intelligence that a minister...refers" to you? Do you believe you don't have the capacity to independently launch such a review of the Zhang case?

Craig Forcese: No, we would take the view that the subject matter of safeguarding—and this would include security clearances—remains within our purview under section 8, and we wouldn't rely on a ministerial referral. In circumstances in which there have been ministerial referrals, we don't limit the scope of our review simply to the parameters the minister has suggested through paragraph 8(1)(c). We independently trigger the other aspects of our mandate to make sure there's a full airing of all the relevant materials. We're not like a commission of inquiry, which is confined by the four squares of the terms of reference. We have a wider remit.

Anthony Housefather: In that case, how come you've decided not to launch an investigation into the Zhang case?

• (1710)

Craig Forcese: Well, to be clear, the decision has not been not made, I shall say. The matter is in the public eye. I will say that, in relation to an investigation that touches on the conduct of an individual, our priority is to assess the conduct of government actors. That's our remit: to assess the conduct of government actors. We are also preoccupied in any instance that might involve an individual in which.... By reason of procedural fairness, we don't want to get into an assessment of their conduct in circumstances in which they have no opportunity to be heard or to provide input. Our focus is squarely on government conduct.

In a circumstance like this, in which we are conducting a review, we would be looking at systemic issues and not simply the specifics of any one case. This is because we have the crosscutting ability to follow the thread in a review mandate, an ability that doesn't exist on our complaint side.

Anthony Housefather: Of course, I completely understand. Your issue would not be Ms. Zhang herself. Your issue would be whether there was a systemic flaw in the processes leading to the fact that information related to a fraud—assuming the fraud is substantiated—was not shared or was disregarded. I'll leave it to you, but it sounds quite serious.

Can I come to the question Madame Dandurand asked about centralization? It seems relatively surprising to me that any department—the deputy head or whatever we're calling the person who has supervisory authority of the department related to this issue—could grant clearance to an individual despite the fact that the

RCMP or CSIS may have advised them not to. I know they don't say, "Don't do it," but they could have provided information that would have led to the average person saying that it should not have been provided.

Would you agree with me that there should be at least some contemplation that—in the event that the deputy head is choosing to ignore a recommendation or important factual information from the RCMP and CSIS that would otherwise lead to a clearance not being granted—they should need to have the authority of a minister, maybe the Minister of Public Safety, to do that?

Craig Forcese: I don't have any position on the policy merits as to what should happen in those sorts of circumstances. I can, though, note that in the 2014 standard on security screening, which is the one we've been most involved in because, of course, it has been in existence for some time, there is a certain primacy given on the security assessment.

The balancing of equities has been a task undertaken by the deputy head, who has to offset the security preoccupations that might be communicated in a security assessment, as against other equities. It seems, in those circumstances, that the Treasury Board made the decision to ensure that a full airing of pros and cons, and not simply being driven by the security services, would determine the question of clearance.

Anthony Housefather: I understand that, and I assume that the 2025 changes that have been made grant even more discretion with respect to the deputy head, because now you have to consider it from an equity framework as well. I understand the balance that has to be made, but it seems our country is moving more toward an understanding that we want to be safe and that we want to keep Canadians safe. What might have been the position a few years ago about the balance.... I think the balance in the minds of most Canadians has shifted, which is why we have such a flurry of justice and public safety bills coming before the House of Commons these days.

Do you not believe that in the current climate, the current world, we should be considering the idea that, should the advice of the security services be disregarded, there must be some higher threshold, with some centralized body, at least to review the decision of the decision-maker in the individual ministry?

The Chair: That's another great question, but there's no time to answer.

[Translation]

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

Claude DeBellefeuille: The question was so interesting, Mr. Chair, that I would venture to ask for a written answer. It's always frustrating to have only an hour to spend with such an exciting and informative witness panel.

Mr. Dufresne, from a legal or regulatory standpoint, what would have prevented Global Affairs Canada from requesting a reference from the commissioners of the Public Service Commission of Canada, who determined Ms. Zhang's fraud? They knew very well that the employee was going to do an internship at NATO, which, according to what we learned, required secret, not top secret security clearance. Did a law or rule prevent Global Affairs Canada from calling the commission, telling it that they were about to recommend an intern and asking if there was anything in her file that was amiss and would prevent them from sending this person to NATO?

From what I understand, the security clearance is shared between the country of origin and NATO. So I'm trying to understand what could have been done differently.

• (1715)

Philippe Dufresne: In fact, this question comes up often and I ask it myself. If we say we cannot disclose the information, we need to identify which section prohibits us from doing so, or what we consider to be the limits of our authority—in other words, what prevents us from doing so.

The Privacy Act provides for the exchange of information in certain cases, for example where the public interest outweighs the impact on privacy. So, would that apply in a case such as this? Are there other possibilities for sharing information under other sections? If I am told that it cannot be done or that it has not been possible to do so, I would ask what the perceived obstacle is. We could then discuss that obstacle. Is it really an obstacle under the act? If so, does it need to be amended, or are there ways of doing this transparently or through agreements with the departments?

Claude DeBellefeuille: Could we conclude by saying that Global Affairs Canada did not consult the commissioner or his team to ensure that, by requesting this information from the Public Service Commission of Canada, the department was not contravening any laws or regulations?

The point is that we must be rigorous when assigning a secret security clearance, particularly when sending a Canadian woman on an internship to an organization such as NATO. I understand that there is nothing to prevent this, but ultimately the responsibility lies with the department. It must ensure that, when granting a security clearance, it has utilized all the necessary tools at its disposal, including the commissioner's services.

The Chair: Thank you, Mrs. DeBellefeuille.

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

[English]

Blake Richards (Airdrie—Cochrane, CPC): Thank you.

I appreciate your being here to share your expertise with us today. It's a very concerning matter, one that we all want to see avoided in the future.

To that end, there were a couple of questions put to you that couldn't be answered, given the time. In particular, I'd like to return to Mr. Caputo's question. Do you recall the question, or do I need to summarize it for you?

Craig Forcese: A summary would be helpful.

Blake Richards: He essentially laid out some of the facts that are known about the case. If I were to rephrase the question, I would say this: Was this a failure of the processes in place, or were mistakes made? Essentially, what can we learn from this? I guess that's the question I would ask. Was there a failure in the processes themselves, were the processes not followed or was it a bit of both—based on the facts that you do know about it?

Craig Forcese: It's a question I can't answer, not having conducted the review work that would be necessary to provide a material response.

In terms of the broader issue about processes, on whether they were followed or the processes themselves were somehow deficient, that's the sort of meat and butter of what we do at NSIRA when we look at systemic issues within a department and increasingly across departments. We would always predicate that, though, on a substantial factual record.

One of the issues mentioned before was the duration of our reviews. The duration of our reviews is often tied to obtaining the information that we require to conduct a high-fidelity exercise. It's not just government information that the government itself feels is relevant; it's to assure ourselves that we have everything we believe is relevant. We will take the time necessary to perform this function and then validate it.

Blake Richards: In your opening remarks, you mentioned three areas of concern. The third one was about some of the methods themselves. This ties to what I was asking you. You mentioned that you had seen methods that certainly raised concerns as to the suitability. Do you want to give us some examples of what you're referring to when you talk about that, and if you see how it might not necessarily tie to this specific situation but would tie to other situations like it as a result of some of those concerns?

• (1720)

Craig Forcese: In terms of review work in this space on internal security, our focus has been on CSIS and CSE, which operate in a top secret environment. With enhanced top secret, there's an obligation to use, under the Treasury Board standards, the polygraph. Our focus has been on the polygraph as an adequate tool to satisfy concerns about the prospective loyalty to Canada of an individual. We have both raised concerns about the accuracy of the polygraph as an instrument, concerns about how it's being used that might compound concerns about this accuracy and concerns about how it might be squeezing out a focus on other methods that would be the sorts of investigative tools one would use to answer the question about prospective loyalty to Canada.

If you're asking in another context, in which techniques are at issue other than the polygraph, or whether there's been an adequate consideration of other methods, in our complaints work we look at, for instance, whether obvious interviewees who should be contacted in relation to establishing whether there's adverse information have been contacted—or haven't, in which case there's a question as to the thoroughness of the investigation. We will look at those sorts of considerations.

Blake Richards: Okay.

Is it your opinion that, at the current time, some of this thoroughness is lacking?

Craig Forcese: There have been instances in our complaints work in which the answer would be yes.

Blake Richards: Do you have concerns that we could see other instances like the type of incident we've seen occur as a result of this lack of thoroughness?

Craig Forcese: I don't want to be put in a position of speculating without an adequate factual record, but in scoping a review in this space, in terms of our methodology, this would be one of the key considerations: If there is a problem, what is its impact, and is it likely to recur?

Blake Richards: Okay.

Mr. Dufresne, I know—

The Chair: I'm sorry to interrupt, MP Richards, but that's all the time we have for this opportunity.

[Translation]

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

[English]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): I'm going around in circles trying to figure out NSIRA's role in this whole thing.

I believe this inquiry was instigated by the Conservatives in response to the concern with respect to the Zhang case that there was insufficient security. Whom did they blame? Surprise, surprise—“It's the minister; we'll throw him under the bus.” We then started looking at who is actually responsible for the security screening. The Treasury Board sets standards for security, and then the departments do the actual screening, and CSIS is involved. Then NSIRA comes along, and I have to admit that before today, I never knew you existed.

On your website, it says, “As Canada's independent agency, NSIRA has a broad mandate to review any activity carried out by a federal department related to national security or intelligence.”

I don't mean to put you on the spot—I do and I don't—but should we be going after you? Is the fact that there was insufficient security your responsibility?

I'll come back to that, because you said you've made recommendations on polygraphs and the government has ignored you anyhow. Maybe you've been given a power to make recommendations without the ability to get the government to act on those.

On that comment, are you the villain in this? Did you not adequately go over the government's security recommendations?

Craig Forcese: We're an auditor. We retrospectively audit the performance of the Government of Canada in the national security space.

We were created to overcome the barrier that secrecy otherwise imposes on, not least, other officers of Parliament and parliamentarians in order to provide assurances that the conduct of the security agencies is compliant with the law as reasonably as necessary.

We have a staff of 60-plus individuals. Our mandate is the entire national security apparatus. We conduct 12 to 15 reviews each year. We prioritize reviews according to a series of criteria, which include the risk posed by the activity that we're reviewing, and we have a stable of public complaints that are brought our way.

We sample the activities of the Government of Canada. We're not in a position to review every single activity the Government of Canada performs in the vast apparatus of national security.

In the security screening space, we have been deeply invested for the last year and a half in immigration security screening. As I mentioned, we have a special report that will be tabled in Parliament imminently. We have also embarked on a separate review of the immigration screening process writ large. The special report will concern CSIS, and then we're looking more broadly at immigration screening within the government system writ large.

In terms of our capacity to give assurance, as an auditor, we focus on the high-risk enterprises, and amongst the reasons that we will look at something are circumstances in which parliamentarians—and we very much value the relationships with parliamentarians—tell us it is something we should prioritize. We take that back, and with our plenary membership, we will decide the scope of any review.

• (1725)

Marcus Powlowski: On this particular...well, on any issue, given the polygraph thing that you've made recommendations on nine times and the government has ignored nine times, I take it the legislation gives you the role of auditor, but there's no obligation for the government to listen to you. That's number one.

Number two, when you do make recommendations, is there an obligation for the government to respond to your recommendations?

Craig Forcese: Yes, we make recommendations. We don't have any power to compel anyone to do anything.

In terms of the outcomes of our reviews or investigations, the practice has been to get responses to our recommendations, and we now have a protocol in which we follow up thereafter as to whether our recommendations have been implemented.

In some cases, we go back and re-review. In many cases, by legislation, we are obliged to review certain topics annually. We now have a corpus of material in which, over the course of years, we've built a considerable record of reviewing a common practice, including in the Security of Canada Information Disclosure Act, another vessel by which the Government of Canada can share between silos national security-related information. It's not just the Privacy Act.

[Translation]

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

Given the time, I think it is time to thank you, witnesses, for preparing your presentation and for coming to take part in this meeting with us. We wish you a good rest of the day and thank you once again for everything you have done to help us.

We will now suspend the meeting for a few minutes to allow other witnesses to arrive.

• (1725) _____ (Pause) _____

• (1730)

The Chair: We are resuming the meeting.

We will begin the second part of the meeting with two witnesses, to whom we extend our welcome.

Firstly, from the Department of Foreign Affairs, Trade and Development, we welcome Ms. Tara Denham, assistant deputy minister responsible for consular affairs, security, legal affairs and protocol, and senior representative for hostage issues.

We also welcome, from the Department of National Defence, Brigadier-General Liam Cox, director general of defence security and chief security officer.

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

Tara Denham (Assistant Deputy Minister, Consular, Security, Legal, and Protocol Branch, and Senior Official for Hostage Affairs, Consular, Security, Legal, and Protocol Branch, Department of Foreign Affairs, Trade and Development): Thank you, Mr. Chair.

Thank you for inviting me to address the committee.

My name is Tara Denham and I am assistant deputy minister responsible for the consular, security, legal and protocol branch at Global Affairs Canada. I am responsible for overseeing security matters for our department, both at home and at our 182 missions abroad. This includes, in particular, our participation in the Government of Canada's personnel security program.

As an investigation is currently under way into a specific matter before the committee, I will not comment on the details of that case. I do, however, welcome this opportunity to discuss security clearance processes more broadly and the lessons that can be learnt from them.

As you heard on Monday, federal departments, including Global Affairs Canada, carry out security clearance vetting of staff in accordance with the government framework established by the Treasury Board Secretariat to ensure that clearance processes are applied consistently, rigorously and fairly across all departments.

• (1735)

[English]

Global Affairs Canada is a department of approximately 15,000 employees. Each year, we process roughly 3,000 personnel security screening requests for employees located both in Canada and at missions abroad. The baseline security clearance requirement for Canada-based employees is secret. We screen to the level of top secret for any Canadian employees serving abroad. This is due to the

nature of their duties and the operating environments in which they work.

Separately, when NATO is interested in hiring a Canadian, Global Affairs Canada serves as Canada's national security authority for NATO. This means that, based on a negotiated agreement, we work closely with NATO to process security clearances for Canadian citizens applying to work at NATO who are not Government of Canada employees. These clearances are processed in accordance with the Government of Canada security screening framework established by the Treasury Board Secretariat. We process on average 45 security clearances each year for Canadian citizens to be employed by NATO.

For secret level clearances, the process includes a security assessment provided by CSIS, a criminal record check conducted by the RCMP and a financial record check conducted by Global Affairs Canada. As the hiring organization, we work closely with them, but NATO is responsible for establishing the reliability of the candidate through positive identification, reference checks, review of employment history, interviews and any other processes conducted in advance of employing an individual. Based on the results of these assessments, Global Affairs Canada makes the final decision on behalf of the Government of Canada to grant or deny a security clearance.

Canada and its security partners take personnel security screening very seriously. We also know the threat landscape is evolving, as is the information landscape that exists around people who apply for positions requiring security clearances. This means that our employment and security-related processes and protections must evolve with the landscape we work within. To do so, we work closely with NATO and Five Eyes partners, as well as security partners across the Government of Canada and the Treasury Board Secretariat, to share best practices and coordinate approaches to personnel security screening in our efforts to protect our people, our information and our assets.

It is important to bear in mind that personnel security screening is one component of a broader, more robust organizational security ecosystem. Security risks are also mitigated through complementary measures, including security awareness programs, compartmentalizing classified information based on a need-to-know principle, reporting obligations, access controls, management oversight and ongoing risk management practices. Together, these measures help organizations make informed decisions, identify concerns early and foster a culture of security and accountability.

Based on our dedication to continually review and improve our security screening practices and to work closely with NATO and other allies when security incidents occur, Canada continues to be a trusted partner. Canada's relationships with NATO and NATO allies remain strong. In addition to our work with NATO and allies, Global Affairs Canada is committed to working with Treasury Board Secretariat and the Government of Canada colleagues to continually assess the strengths of our processes and areas for improvement.

Thank you, Mr. Chair. I look forward to the committee's questions.

• (1740)

[Translation]

The Chair: Thank you, Ms. Denham.

We shall now hear from Brigadier-General Liam Cox.

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

Brigadier-General Liam Cox (Director General Defence Security and Chief Security Officer, Department of National Defence): Good evening, ladies and gentlemen.

[English]

I am Brigadier-General Liam Cox, and I am here representing National Defence.

As director general defence security, or DGDS, I support the vice-chief of the defence staff as the functional authority for security in the Department of National Defence and the Canadian Armed Forces. I am also appointed chief security officer by the deputy minister and chief of the defence staff. For DND and CAF individuals, I am delegated to grant, suspend, reinstate, deny or revoke security statuses or clearances. I can also temporarily deny access pending investigations.

My office is broadly responsible for protecting, promoting and supporting security in DND and CAF activities. Specifically relevant tonight is the fact that I am the operational authority for security screening and the insider risk program within DND and CAF. I ensure the integrity of the security screening function as a core element of defence security.

For context, DND and CAF issue reliability, secret, top secret and enhanced top secret clearances. With respect to Canadians who work in NATO, DGDS is responsible for the security screening of DND and CAF personnel. In that situation, DGDS issues, confirms and monitors the validity of those personnel security clearances.

[Translation]

Thank you.

The Chair: Thank you very much.

We shall now move on to questions from members, starting with Mr. Lloyd for six minutes.

[English]

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

Thank you, witnesses.

In the context of the case that has brought us here today, I understand you can't speak about specifics of the case, but it's been speculated by some security experts that this person may have been compromised after they received their security clearance.

Can you both describe to me what processes, if any, there are for continuous monitoring to ensure that somebody who has received a security clearance does not become compromised after receiving this access to the Canadian government?

Tara Denham: I'm happy to begin, if you'd like. Thank you for the question.

In my opening comments, I referenced the broader security culture that we need to continue to inculcate across our organizations. Yes, there's the security screening, which is the first step, but really, a lot of steps are then taken, including compartmentalizing the information and making sure that people only have access to information—

Dane Lloyd: I'm sorry to cut you off. I understand that those are all good security risk management processes, but I'm specifically talking about individuals who have received a security clearance. What efforts, if any, are undertaken to continuously monitor these people to ensure that they don't later become security risks?

Tara Denham: There are two ways we do that.

One of the strongest is making sure that the entire organization, including colleagues, managers and people who work together, understands that if you see something, you say something. If someone's behaviour is changing, report it.

We also bring a lot of awareness to individuals about some of the threats they may encounter. For example, internationally, we all know that we're exposed to espionage threats, so we spend a lot of time making sure that our staff understand what this could look like and what types of trends we're seeing so that we can bring their awareness up.

One of the strongest ways to continue to monitor and identify where there may be weaknesses is having colleagues around who report on incidents.

Dane Lloyd: Go ahead, Brigadier-General Cox.

BGen Liam Cox: I'll build on what Tara said. She spoke to the security layers, but there are specific activities that we can do for screening if cued, be it because somebody said something or there was a change-in-circumstance report, which is a vehicle to communicate either a behavioural change or changes in a person's life, that raised doubt or raised a review for cause. There are mechanisms we can use to respond to cueing.

As for your point about continuous assurance, it might have been spoken to on Monday that the new directive on security screening talks about it being not just a one-and-done check every five or 10 years but, inside this cycle, a reviewing or running of criminal checks or credit checks on a cyclical basis to see if anything can be flagged that way.

Dane Lloyd: I'm quite concerned, because we're basing this on people who report their colleagues or self-report, but I think people have very personal private lives.

I wanted to ask the Privacy Commissioner this when he was here: Is there anything in the Privacy Act that prevents departments from doing their due diligence when they have already hired somebody who has gone through the clearance? Is there anything in the Privacy Act that prevents departments from checking in on people who might be of concern?

• (1745)

BGen Liam Cox: There are guidelines and guardrails, if you will. There are checks we can do on a continual basis, and there are limits to those. Whether in response to an investigation or a need to resolve a doubt, there's a different set of tools that can be applied to find the information that we may need to draw a conclusion if there's adverse information.

Dane Lloyd: Are there Privacy Act limitations on continuous monitoring of people who have security clearances?

BGen Liam Cox: Yes. The limitations are more the guidelines in that when we approach someone to do a security clearance, they give us consent to seek the information that we need to give them an initial clearance. That's in keeping with the guidelines on privacy. They agree to disclose the information that will help us to grant the initial clearance. If adverse information is found later, then we need to conduct the investigation using the tools that we need to resolve that doubt.

Dane Lloyd: Okay. Thank you.

I'll pass my time on to my colleague Mr. Caputo.

Frank Caputo: Thank you, Mr. Lloyd.

I'm a bit confused. If somebody is going to work at NATO as an intern in Belgium, what level of security clearance do they need?

Tara Denham: As was noted on Monday, I believe, the typical clearance level for NATO—again, not speaking to this specific case—would be a secret clearance level. To give you an example, I noted that we do about 45 clearances per year to support NATO when they're hiring individuals, and about 85% of those are secret. Some are top secret, as NATO requires, and this is based on the position they're being hired for. I also want to clarify that NATO, as the hiring organization, defines what the clearance level is.

Without getting into the specifics of the case, I noted that this was not a Government of Canada employee. This was not somebody who was sent to do an internship on behalf of the Government of Canada. This was an employee who was hired by NATO.

Frank Caputo: I'm thankful for that clarification but, at the end of the day, there's still a Government of Canada security clearance on somebody who had been flagged for fraud and may have had other flags.

I think Mr. Lloyd's point, if I may be so bold as to try to summarize it, is that somebody may get a security clearance and then be found guilty of fraud. Maybe it's not in the legal sense, but they were within the Government of Canada, and they were flagged as providing fraudulent information.

What mechanisms are there so that the left hand knows what the right is doing? In other words, is there a mechanism by which somebody has lied on their CBSA application, and it goes, "Hey, they've got a secret security clearance. We should know this."

The Chair: The bad news is that we need to move to MP Sodhi. The good news is that there will be a turn for you, I believe, very soon for the answer to be heard.

We have MP Sodhi for six minutes, please.

Amandeep Sodhi (Brampton Centre, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for being here today.

I'll direct my first set of questions to Ms. Denham.

When deciding whether to grant a security clearance for an applicant, what sort of information does your department itself investigate and assess? Also, what information is provided to you by external agencies such as CSIS and the RCMP?

Tara Denham: For a secret security clearance, as was noted on Monday—but to be clear on the information that is required—it includes confirming the identity of the individual. Therefore, I confirm your driver's licence, education, professional credentials, and personal and professional reference checks. That's done by the hiring manager; whoever that hiring manager is, they would do those things.

In terms of the security professionals, these relate to the financial checks for Global Affairs, and we do those using Equifax. We also work with the RCMP, and the criminal record check is done by the RCMP. The security screening, as CSIS mentioned, is focused on threats to national security and loyalty to Canada and is done by CSIS.

It is really important and was noted on Monday that you take all of that together, and you make the final assessment. If no adverse information is presented, then the secret clearance would be granted. If there is adverse information, you have to consider what that adverse information is. Then, as we've noted, security clearances are about managing risk. We have to think about what those risks are. What is the context of that, and do we have to pursue further discussions or interviews with the individual?

• (1750)

Amandeep Sodhi: As a follow-up, do you believe there are any gaps in the processes that are currently used? If you do believe there are gaps, how could we improve on these?

Tara Denham: I made mention of working really closely with Five Eyes, NATO and other government departments. We're always looking at what can be improved, because of the rapidity with which the threat environment changes.

I would say that, more often than not, the security screening policies that governments have are pretty similar in terms of those steps that I described. We see that a lot of the lessons we learn because of different cases and scenarios are around those criteria that we should think about when we're doing those assessments. This is a lot of the learning that we do.

I would say that some of the areas that have been identified, as noted before, have also been integrated into the Treasury Board policy of 2025 but, over the last number of years, Internet inquiries have become identified as a tool that would be very important. The Treasury Board policy now makes that mandatory for people seeking top secret, but it's not required for secret. In terms of our work with NATO moving forward, we will now include Internet inquiries into that, again using the tools that are available to us.

There have also been some important questions, and the distinction and what is coming out is that there is the security process and the security files that are looked at, and there are also human resource files, and those are distinct. Human resource files are not necessarily included in financial, criminal or security checks. There are important questions being asked, and we're always open to learning in terms of respecting privacy and whatever other mechanisms are required, as well as where they could be improved.

Amandeep Sodhi: On Monday, we learned that when an individual transfers between departments, their clearance is either verified or redone by the new department.

In your experience, is it more common for a transferring employee's clearance to be simply verified, for the security screening process to be restarted or does it depend?

Tara Denham: It really depends. There is a lot of movement between organizations. We all have the same requirements because it's guided by Treasury Board in terms of the basis on which those security clearances were granted. It depends on the job, which defines what you're being hired to do.

Let's say that somebody is moving from the Department of Fisheries and Oceans. They have taken their security process reviews and they've assessed it. If they are coming into Global Affairs, the sending department would be able to share that file with us and flag if there was any adverse information at any point. Then we would make the assessment on whether we should look into it further. Some of the threats and issues an employee of the Department of Fisheries and Oceans has may not be the same as some of the issues we may be concerned with. That's when we would decide whether we are going to accept it as is or whether we will redo it. We don't always have to start from the full thing, but for example, if a criminal record check hasn't been done in a year or two and there's a gap in employment, we could decide to run that again, or we may want to run a financial credit check or something.

It really depends on when the security clearance was granted, whether there was a gap in employment that they can't account for and what they are being hired to do now. We may want to ask further questions.

Amandeep Sodhi: Beautiful.

Mr. Chair—

The Chair: I'm sorry. There are only 10 seconds left.

Thank you, MP Sodhi.

[Translation]

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

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

I would like to thank the witnesses for being here.

Ms. Denham, I very much appreciated your testimony because it has clarified things for me. I understand better now. You used a word earlier that really struck me. You said that you use the security vetting carried out by the Canadian Security Intelligence Service and the RCMP, but that it is not standard practice in your procedures to carry out a systematic check of the human resources file of an employee who has worked in, and has a history of working in, various departments, and for whom you must determine or recommend a security clearance level, for example at an organization such as NATO.

From the outset, there has been much discussion about the creation of central files, particularly for individuals requiring a secret or top secret security clearance. Is there any obstacle in the process that prevents you from consulting the human resources file because you believe the Privacy Act prohibits you from doing so?

In your process, do you consult the Privacy Commissioner for advice and to really delve into the human resources file? For example, in a case such as that of Ms. Zhang, could you have checked whether there had been any mention of fraud in her employment history at the Public Service Commission? If you'd had access to her human resources file, right there and then, there would probably have been a negative comment that would have led you to investigate the matter further.

Isn't access to the human resources file part of your procedures? Should consulting an employee's human resources file, in essence, be something that needs to be formally established?

• (1755)

Tara Denham: Thank you for the question.

[English]

There are two parts to that. The first part was whether there is a systemic, centralized HR system.

[Translation]

Secondly, you asked me whether there were any legal obstacles.

[English]

Let me first speak to the centralization of human resource files.

A colleague noted on Monday that we have a centralized performance management system within the Government of Canada. I think we can all acknowledge that there are always opportunities to improve this. It's not exhaustive. It's more talking—

[Translation]

Claude DeBellefeuille: Excuse me, but the interpreter missed a small bit. Did you just tell me that there is a centralized government database and that it is either not being used or is poorly used?

[English]

Tara Denham: I will not switch back and forth. I'll speak in English so that the interpretation works clearly.

Right now, what is centralized is a performance management system. This is really about “what are your objectives for the year and did you do a good job?” That is across the Government of Canada, and that can move with you throughout your career.

[Translation]

Claude DeBellefeuille: I understand that the results of performance appraisals are centralized. However, employees' human resources records are not centralized. So, if an employee has committed a serious offence or received a disciplinary warning, this is not recorded in the central file. Have I understood this correctly?

[English]

Tara Denham: Yes, that is not centralized. In terms of obstacles, I'm not a human resource expert, but I understand that human resource files can be held for only two years unless there has been disciplinary action. Again, even if there were a centralized data bank on the human resource file of an individual, my understanding is that HR files, in terms of any actions or issues that arose, are not held beyond two years from the incident.

This would be one obstacle, but by and large, a lot of the questions have come to privacy issues. This is an excellent question that can be explored, but I'm not the expert on that.

You asked, “Is there a centralized system?” No, but any centralized system would have to be extremely careful to protect privacy considerations for the individuals, and that would be a concern.

[Translation]

Claude DeBellefeuille: The Privacy Commissioner told us earlier that there was no law or rule preventing an institution from requesting information if it could prove that national security was at risk. I understood from his testimony that there was no formal consultation process to seek the commissioner's advice when assessing, for example, a secret or top secret security clearance, to determine whether one could access human resources files or go further and disclose the information obtained. There does not appear to be a practice within your department of seeking this information.

• (1800)

[English]

Tara Denham: What I would say is, first—

The Chair: Answer shortly, please.

Tara Denham: Okay.

If there is a centralized database on human resource files, there would be privacy considerations that would have to be taken into account, but there are means to share HR information when it comes to national security. There are means to do so. In terms of whether we seek out that information, as I mentioned, a hiring manager looks at the education, but also at professional and personal references. When somebody is hired by NATO, NATO would undertake this process.

For me, if it were an employee of GAC and I was hiring them, I would undertake that. Absolutely, like any organization, I can call and I can do references, and I think the larger obstacle there is the consistency in the way managers conduct reference checks—

The Chair: I'm sorry to interrupt, but this is an appropriate time to switch to MP Caputo.

Mr. Caputo, you have five minutes, please.

Frank Caputo: Thank you, Mr. Chair.

Ms. Denham, I'll pick up where we were.

Do you recall my question, or do you want me to repeat it?

Tara Denham: I noted the link between human resource files and security files.

Frank Caputo: Yes. I was talking about one hand not knowing what the other hand is doing. I mean by that Mr. Lloyd's point in which somebody could obtain a security clearance and then have information surfacing that would nullify or cancel that security clearance.

Is there a mechanism by which somebody who has been found guilty of fraud, for instance, on a government application.... How is the information communicated? Does it get run against a database of, hey, this person has a security clearance? I don't know the intricacies of how these things work. I'm sure AI can do a number on it, but if somebody has a security clearance and they have a finding of fraud, is there any automatic alert? Is there a red flag? How does that work?

Tara Denham: There is no automatic alert. In terms of the process, when we're doing reviews for security clearances, particularly for criminal and security checks—a security check is for threats to national security—for the Public Service Commission and any findings related to that, such as any potential findings of fraud, it is an administrative decision. It is not a legal finding. This would not bring up a criminal record check. Does a finding of fraud, if somebody applied different ways or had issues within the Government of Canada, reach the level of a threat to national security? It may not reach the criteria.

As I said, there are lessons we learn in different cases in terms of what some of the criteria we should ask about are. In terms of automatic flags from the Public Service Commission or HR files that are linked to security files, there are distinctions between human resource files and security files.

Frank Caputo: Therein is the gap, I suppose, that I think Mr. Lloyd was trying to explore and that I'd like to explore.

Let's say you have a secret clearance, which I believe is five years in duration. Is that right? Is a secret clearance good for five years?

Tara Denham: Yes.

Frank Caputo: Okay. If somebody has, say, a breach of a driving prohibition—which is something you can go to jail for and is a provincial offence oftentimes—that's an honesty offence. It's a breach of a court order. In my view, that's a pretty big deal if you have a secret level clearance. From what you're telling me, there's nothing that would necessarily pick that up and show that somebody breached a court order one year in. If they're not a police officer, probably nobody will know, especially if somebody keeps to themselves.

Do you see the gap I'm trying to get at?

Tara Denham: Let me clarify. What I was describing was when we're doing a security clearance for somebody who is not currently an employee of the Government of Canada. You're describing somebody who has been granted security clearance and the ongoing monitoring.

• (1805)

Frank Caputo: That's what I think Mr. Lloyd was trying to get at. It's somebody who has been compromised after the fact.

Tara Denham: This is what we were talking about when there is a review for cause. Within Global Affairs, when we get hired, it is made very clear to us that not only is it “see something, say something”, but we also have a duty to report. If there's a change in circumstance in our lives that could have an impact, you have those.

There are means by which there are duties and obligations to report a change in circumstance. Depending on what that is—depending on the job somebody holds—there could absolutely be a review for cause.

Frank Caputo: I'm sorry to cut you off. That's not what I'm getting at.

A nefarious actor isn't going to put the spotlight on themselves. Do you get what I mean? They're not going to say, “Hey, please review my security clearance.” This is the whole point, though. It's

that there are grounds to review the security clearance. There's a basis to review it, but nobody knows that. Something has happened over here, but they don't know it over there, even though over here is where the security clearance is. Am I being clear?

Please, go ahead.

BGen Liam Cox: Maybe I could build on that, Mr. Chair.

If the threshold is criminal or something that would appear on a criminal record check or a CPIC kind of thing, with the new DSS there is a cycle of review running CPICs inside the window of....

As the Government of Canada, we're moving toward some sort of continuous monitoring assurance. The next bound, which we're trying to map toward, is some sort of “real-time alert”, where.... Currently, the RCMP provides that cueing to the department. It's not when they run the check. If we advise them that someone is our employee, they can see if somebody has been pulled over by the police, etc., depending on the threshold. That would be entered in CPIC.

Yes, on what you're mentioning, in part of the DSS we are moving to a place where we have that monitoring or that continuous assurance, so we aren't relying only on people to self-disclose.

The Chair: I'm sorry, MP Caputo.

[Translation]

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

Jacques Ramsay (La Prairie—Atateken, Lib.): Good morning. Brigadier-General Cox and Ms. Denham, thank you for taking part in this meeting and for providing us with your insights.

I have an initial question for you, Ms. Denham. It is just to clarify something. You told us that it was the North Atlantic Treaty Organisation, or NATO, which was responsible for its vetting process—that is, the interviews and background checks. Does that mean that Global Affairs Canada was not involved in any way?

As you are not authorized to discuss a specific case, I will ask you the question in general terms. When NATO carries out this sort of vetting, does it liaise with you? Does it obtain information from you, or ask about the security clearance that was previously granted?

[English]

Tara Denham: I'll clarify. We have a negotiated agreement with NATO in terms of the steps that need to be followed, and those same steps are the ones that are set out in the Treasury Board policy. They are about confirming identity, education and professional credentials; doing personal and professional reference checks, as well as the financial and criminal inquiries; and assessing the threat to national security.

Within any security screening process, it is the hiring manager who leads on confirming the identity, the education, and the personal and professional experience. That is part of our relationship with NATO. Just as there are across Global Affairs, there are forms to fill out. We are very clear on the information that is required, and the hiring manager completes that information.

If there is any adverse information, they are required to tell the security officials because, at the same time, Global Affairs Canada is pursuing the other checks that are required for a secret security clearance. We do the financial check using Equifax. We work with the RCMP to do the criminal record check, and we work with CSIS to do the security check.

When all those checks are done, they have to be confirmed by those who are conducting those checks, and Global Affairs is responsible for pulling them together. If there is no adverse information, then we issue the security clearance, but we hold all the documentation of those respective individuals who did the requisite security checks.

[Translation]

Jacques Ramsay: Last Monday, we heard about things that could be done in addition, or improved upon, including, among other things, the much-discussed Internet monitoring. I respectfully suggest that any budding spy would clean up everything on the Internet—you don't have to be Jason Bourne. So, is this sufficient in the specific case of foreign threats or foreign interference? What more could be done?

My question is addressed to both of you.

• (1810)

[English]

BGen Liam Cox: I would also agree that there are limits to what can be done with a surface-level Internet check. Of course, if somebody has any statecraft, they can obfuscate their behaviour, and we wouldn't find it with a surface-level Internet check.

That's why it isn't the only thing—and can't be the only thing—we use to try to get an understanding of who the persons are who present themselves and to try to understand if there are vulnerabilities or maybe things they haven't yet disclosed.

There isn't one thing that assures any kind of certainty as to understanding who a person is when they present. An Internet check can find some things for some people, but yes, your point is extremely accurate. If they don't have their persona online, we won't find it with an Internet check on the surface.

Tara Denham: The only thing I would add is that it is another tool we can use. Yes, there are challenges, but we're using the Inter-

net inquiry along with other lines of information that we gather about an individual.

If we did start to gather information from reference checks, employment history or other aspects and at the same time did an Internet inquiry and could find absolutely nothing that seemed indicative that perhaps it would make sense that they would have an Internet presence, this would be a question that should be asked. You take it together and assess the information. You have to look at the whole picture and decide whether you need to question the individual further.

[Translation]

Jacques Ramsay: If—

The Chair: I'm sorry to interrupt you, Mr. Ramsay.

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

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

Mr. Cox, as I understand it, this is a shared responsibility when a Canadian goes to work as an intern at NATO. It is a shared responsibility to verify and ensure that this person holds a secret or top secret security clearance, depending on the post they will hold.

We are not specialists in security vetting, but the Zhang case strikes us as a serious matter—a lack of competence or rigour, a significant flaw, a major shortcoming in our system.

Can you tell us what impact this has on Canada's image among other NATO countries, who see that a Canadian woman managed to circumvent the entire security vetting process to reach NATO? Do you think our image abroad has taken a hit? How can the Department of Defence rectify this to regain the trust of other countries? In your view, has Canada really tarnished its image with the high-profile case of Ms. Zhang at NATO?

[English]

BGen Liam Cox: I can't speak to the particulars of this case to suggest that it was a large gap, but I can assure everyone that there is no loss of confidence in us with our allies. We build trust by collaborating and being effective in sharing information, as well as by maintaining the standards we have and communicating how we follow them. Hypothetically speaking, unfortunately, insider risk is not a new thing. It's a pervasive problem. We're all dealing with it as allies. A dedicated actor who wants to infiltrate probably can, unfortunately, especially at certain levels. The collaborative approach to make sure that we can catch, if you will, any breaches by the layered security defence is in ensuring that we grant access to only certain areas so that when something unusual occurs, it's noticed.

I would conclude by saying that, unfortunately, all our allies are struggling with the same thing. Our trust is reinforced by sharing with them, continuing to collaborate, sharing lessons observed and working together on insider risk.

• (1815)

[Translation]

The Chair: Thank you very much.

Mr. Richards now has the floor for five minutes.

[English]

Blake Richards: Thanks.

I'll start with you, Ms. Denham. I appreciate that you can't share details about the individual case, but it's been indicated that there is an internal review of sorts happening as a result. I wonder if you can speak to that. Can you tell me the scope of that investigation, the status of the investigation and when we might expect to see results and recommendations that would come from that internal review?

Tara Denham: Thank you, Mr. Chair.

In terms of the scope, we have done an internal review, as was mentioned by the Minister of Public Safety. All of the implicated departments were asked to do an internal review. That has been completed. It entailed going through the case—as with any case, not specifically this one—to make sure the steps were followed. Did we follow the process as outlined? I can say that the internal review was completed. We noted that all the steps were followed.

That pushes us to the second part, which is the focus of this committee: Where are the lessons that can be learned? That's the critical part. As was said, we're all facing threats all the time. We want to extract the lessons. That's what we've worked on with Treasury Board and all the implicated departments, to identify where some of these lessons could exist. Those recommendations have been consolidated. It has been referenced that those are before the Minister of Public Safety. This is because they're broader recommendations in terms of the policy itself.

I want to say that changes to policy are the purview of the ministers, but there is nothing stopping us from making immediate improvements. Those Internet inquiries would be an example of an immediate improvement.

Blake Richards: The recommendations have been sent to the minister. Now it's in his court to determine whether he or the government moves forward with any changes as a result. Is that fairly summarized?

Tara Denham: We participated in a process of identifying recommendations in terms of improvements that could be made to the policy. Again, in terms of Global Affairs Canada, Treasury Board guides that policy, but we all have lessons that contribute to that.

In terms of areas—

Blake Richards: Just so I'm clear, I think you indicated that some recommendations for change had come from what you...and they are sitting with the minister. Is that accurate?

Tara Denham: On Monday the Minister of Public Safety also made reference to the fact that there will be lessons learned and that he will be reviewing the recommendations.

Blake Richards: Okay.

I'll turn to you, Brigadier-General. Correct me if I'm wrong, but it's my understanding that when we have a civilian individual who is looking to work at NATO, GAC is responsible for the security clearance. If it's an individual who's within the CAF or DND, then DND would be responsible for the security screening for that individual. Is that correct?

BGen Liam Cox: That's correct. For DND and CAF members, we would, as a competent—

Blake Richards: I'll let you answer that, but first I want to add to it. In responding to that question, can you indicate how your processes might be different from those of Global Affairs?

BGen Liam Cox: I don't think they would be different at all. We follow the Canadian security requirements.

I say that because NATO itself doesn't have a security screening system. They have an agreement in which partner nations have agreed to a common standard. For us, that means executing our screening activities to grant clearances of reliability, secret, etc. Given that we follow the same process, when we badge someone, although that's not what it's called, or we issue someone a secret clearance, it's to the Canadian standard, which is recognized by NATO.

Blake Richards: Should there be concerns? If something happened with this individual, should we have concerns as Canadians that someone from CAF or DND could potentially be exposed in the same way? Are there changes that you think need to occur, as a result of this incident, to the processes that you have in place?

BGen Liam Cox: I wouldn't say there are changes. It just reinforces the need to be cognizant of the risk. We call it an “insider risk” program, or having a continual, layered approach to make sure that we see any weak signals, indicators and warnings, or behaviour changes that would cue us to look a little further.

It's re-emphasizing the point that we simply can't be successful by looking at someone once every five years or 10 years, because that's not how people are. Things change in their lives. Knowing that those compromises—breaches—can occur, we have to shape our approach, not to say that we'll declare victory and it will never happen. That would be an incorrect approach, but this just reinforces the fact that it's a continual process and we need to look at the “whole of person”, as they say, on a continual basis.

• (1820)

The Chair: Thank you, MP Richards.

We have MP Acan for five minutes, please.

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

Ms. Denham, my questions will be similar and will sound similar or the same, but any responses you give will probably provide good additional information to this study.

When GAC acts as a sponsoring department for Canadians seeking a position in an international organization, is GAC responsible for the decision to grant or deny the Canadian security clearance?

Tara Denham: Just to be clear, when GAC is sending an individual as part of our deployment—we have missions around the world—we are sending an individual who is an employee of Global Affairs Canada, and we screen them to “top secret” because of the work we’re asking them to do. We have the agreement with NATO. When NATO is interested in hiring people from members of the alliance, we have an agreement in place in terms of how to screen those individuals.

Sima Acan: That’s why I used the words “sponsoring department” in imagining that it’s your intern or your employee who is going abroad, but in this individual case, it is not. That was very clear. Thank you so much for enlightening us with that.

Can you walk us through the security screening process that GAC follows when sponsoring or not sponsoring a Canadian seeking a position with an international organization, from the initial request to the final clearance decision? What roles do CSIS and the RCMP—and, where applicable, foreign governments or the international organization itself—play in that process if we consider those processes as two separate processes?

Tara Denham: Okay. If I understand your question correctly, it’s on clarifying again the role of CSIS and the RCMP in the security clearance process.

We work with the RCMP to do the criminal record check, and we work with CSIS to do the threats to national security. CSIS does those security checks. It would be CSIS that can speak to any of the criteria they look at in terms of threats to national security, but that’s who we rely on to do that particular check.

Sima Acan: Is this a different screening process for positions within Canada?

Tara Denham: No. Any security screening process is based on the Treasury Board guidance and the security clearance process. If you’re going to get a secret clearance issued by any department within the Government of Canada, the process and the requirements are the same.

Sima Acan: Does GAC determine whether an existing Canadian security clearance meets the requirements of a position within an international organization if you are sponsoring or in this case?

Tara Denham: The institution that is hiring for a position defines what the position entails and what security clearance is required to hold that position.

Sima Acan: As I understand it now, CSIS or the RCMP provides a security assessment, but the sponsoring department or the hiring department remains responsible for the clearance decision—or is it GAC?

Tara Denham: For any department...I know about security clearance. You’re becoming experts, and it can be very confusing.

Global Affairs is responsible for the security clearance process, the full security clearance, all those steps for anyone we are going to hire in our department.

National Defence and Canadian Armed Forces are responsible for all of their parts. The only distinction is with NATO, because we have an agreement with NATO, as has been articulated. NATO has an agreement with all the allies to rely on the agreed-upon security screening process of the country of origin. In this instance,

we’re not sponsoring individuals to go and work at NATO. The individuals Global Affairs sends to represent us at NATO are top secret cleared, and those are Global Affairs employees.

I hope it’s clear that any department is responsible for completing the security clearance steps. The uniqueness is when it is NATO because of the agreement that we have in place to complete security clearances and work with them to do so.

● (1825)

Sima Acan: [*Inaudible—Editor*] as clearly you stated that you are doing this type of security clearance based on the NATO requirements.

Tara Denham: No. It is all based on the Treasury Board guidelines on security clearance.

Sima Acan: No. I mean when an individual is hired by NATO—

Tara Denham: Correct. It is a request from NATO that they would like to hire an individual, and they require a particular security clearance. We will then follow the steps, depending on the security clearance level that NATO is hiring them for.

Sima Acan: Thank you so much.

The Chair: Very good. Thank you, MP Acan.

Seeing the time, we’ll do three short rounds of two and a half minutes, starting with MP Kirkland. Then we’ll have MP Dandurand and MP DeBellefeuille, and that should be the end of it.

Madame Kirkland, you have two and a half minutes.

Rhonda Kirkland: Thank you, Chair. You have made my day. I thought I wasn’t going to get to ask my question.

Hypothetically, a short while ago, I, Rhonda Kirkland, applied for a position. Let’s say it was at CBSA. However, I committed fraud. I used different names. It was found out. I could not get a position because it was flagged that fraud was committed. Therefore, I didn’t get the position.

A short time later—however long, a year, two years, I’m not quite sure but later—I decide I’m going to apply for a position within NATO, an intern position. When I do that, is Global Affairs, during the screening process—because I understand the partnership now, so I appreciate that. Is it ever looked at that I have been...? Am I red-flagged because somewhere else within the public service for the federal government I have committed fraud?

Tara Denham: In a hypothetical scenario in which—I apologize—you were unsuccessful in securing the employment—

Rhonda Kirkland: It’s my own fault.

Tara Denham: Therefore, you did not get a security clearance. You were not hired, so from a security screening perspective, that would not show up. Where it could show up is—again, I'm not going to speak about NATO—let's say you came to try to work for me, and I was the hiring manager. Depending on the robustness with which I chose to undertake professional references and checks.... It's not an automatic red flag, but if I were able to look through your employment history, perhaps in doing reference checks—

Rhonda Kirkland: It's hard to do that if they don't get hired, though.

Tara Denham: Absolutely.

Rhonda Kirkland: Could this be a gap, then, that could be looked at to be remedied so that, if I were denied in one area of the public service and the federal government, I would be red-flagged with all the names I ever used, including my actual name, when I apply to another branch?

Tara Denham: These are interesting questions about the intersection between security files and human resource files, and what it could look like respecting privacy and other areas to have an ability to use a central database. That's an interesting question.

Rhonda Kirkland: Would you like that?

The Chair: I'm sorry, Madame Kirkland. That's all the time we have.

Let's turn to MP Ramsay.

[Translation]

You have the floor for just two and a half minutes.

Jacques Ramsay: Brigadier-General Cox, I took part in a similar process not so long ago, and I noticed that many of the questions were aimed at identifying vulnerabilities that could be exploited by a third party. Is this also a key consideration in your process within the armed forces?

[English]

BGen Liam Cox: Absolutely. What you're highlighting is, of course, how we're interested in criminality. We're interested in any vulnerabilities or conflict of interest that might lead to someone who has committed something, may be committing something or may have the potential to commit something. I'm using “committed”, but the point that was made was around a vulnerability to be exploited.

It's absolutely fundamental to try to get a sense of the person who presents...if they themselves, because of circumstances, familiar relations or holdings overseas.... Any of those could be used as leverage against them if they were to be granted access to very sensitive information. Are they a desirable target, and do they present, based on their circumstances, vulnerabilities that could be exploited?

• (1830)

[Translation]

Jacques Ramsay: Ms. Denham, you spoke of constantly evolving threats and a landscape that is always changing. As assistant deputy minister at Global Affairs Canada, what are the main recent

risks and threats that security clearance processes should take into account?

[English]

Tara Denham: Are you referring to our individuals? I was confused by the question related to security clearance.

[Translation]

Jacques Ramsay: As assistant deputy minister at Global Affairs Canada, how should security clearance processes adapt? In your view, what should we be wary of and what should the main concerns be?

[English]

Tara Denham: Thank you for the question.

I've mentioned that one of the areas that is very concerning is, of course, espionage and the targeting of individuals. Insider threats have been mentioned. These are approaches many countries try. They try to penetrate all of our organizations and all of our governments, and you all have to be continually aware. Other threats include, of course, cyber and security threats, impersonation of our individuals overseas, the attacking online of our individuals, someone presenting themselves to individuals online and trying to access—

[Translation]

The Chair: I'm sorry to cut you off. That was a little longer than planned.

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

Claude DeBellefeuille: Thank you, Mr. Chair, for your great generosity.

Ms. Denham, having spent my career in management, I firmly believe that the best solutions come from teams—that is, when people on the ground identify a problem. For the purposes of the report, if you had to make a single concrete recommendation—one that we, as your voice, could put forward to improve the security screening process—what would it be?

[English]

Tara Denham: Thank you for the question.

One of the areas we're already working to improve is the Internet inquiry. Right now, it is a requirement for those who are applying for top secret clearance, and we need to put that in place. We are now also going to do that for individuals going to NATO. We have to acknowledge the information environment that is around us and how we can best get as much information as possible that is pertinent and non-intrusive but also helps us make the best decisions.

To be honest—and we've alluded to this—there is always the question of how we can do better to get as much information as effectively as possible. There are interesting questions related to human resource files and employment history that currently are not defined within a security clearance process. There are protections that every Canadian needs to be afforded from a privacy perspective. We have to be very careful about that, but it is an interesting question to see how we could manage that.

[*Translation*]

Claude DeBellefeuille: To conclude, we might suggest that you involve the Privacy Commissioner in your deliberations so that he can advise you on how to safeguard national security while ensuring the confidentiality and sharing of personal data. I believe he is open to advising you on this matter. I therefore encourage you to draw on his expertise and that of his team.

The Chair: Thank you very much for those almost affectionate words, Mrs. DeBellefeuille.

This leads us to extend our warmest thanks also to the two witnesses, Ms. Denham and Brigadier-General Cox.

Before we adjourn, I would remind members of the committee that we will not be sitting next week. The following week, on Monday, October 19, we will examine the revised version of the report on port customs clearance. We will also review the report on Canada's capacity to deport foreign nationals with a criminal record. The following Wednesday, we will continue the examination we began today into security screening processes. The following Monday, October 26, we will begin our consideration of Bill C-236, tabled by our colleague Dane Lloyd, and we will be hearing witnesses. The deadline for submitting amendments to this bill is Friday, October 23, at midday. The following Wednesday, October 28, we will proceed with the clause-by-clause consideration of Bill C-236.

If that is acceptable to you, we will now adjourn the meeting.

Thank you, and 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>